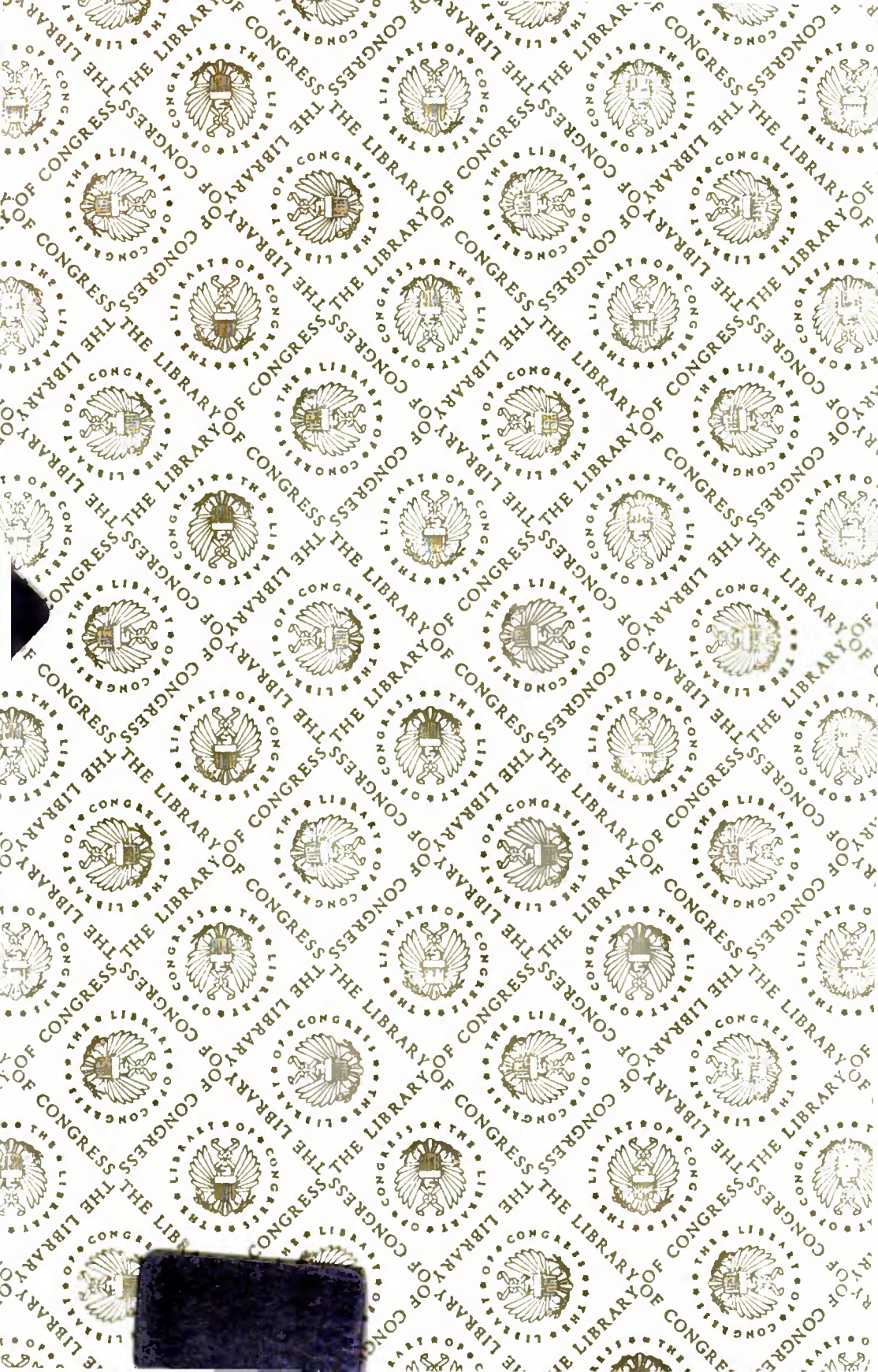
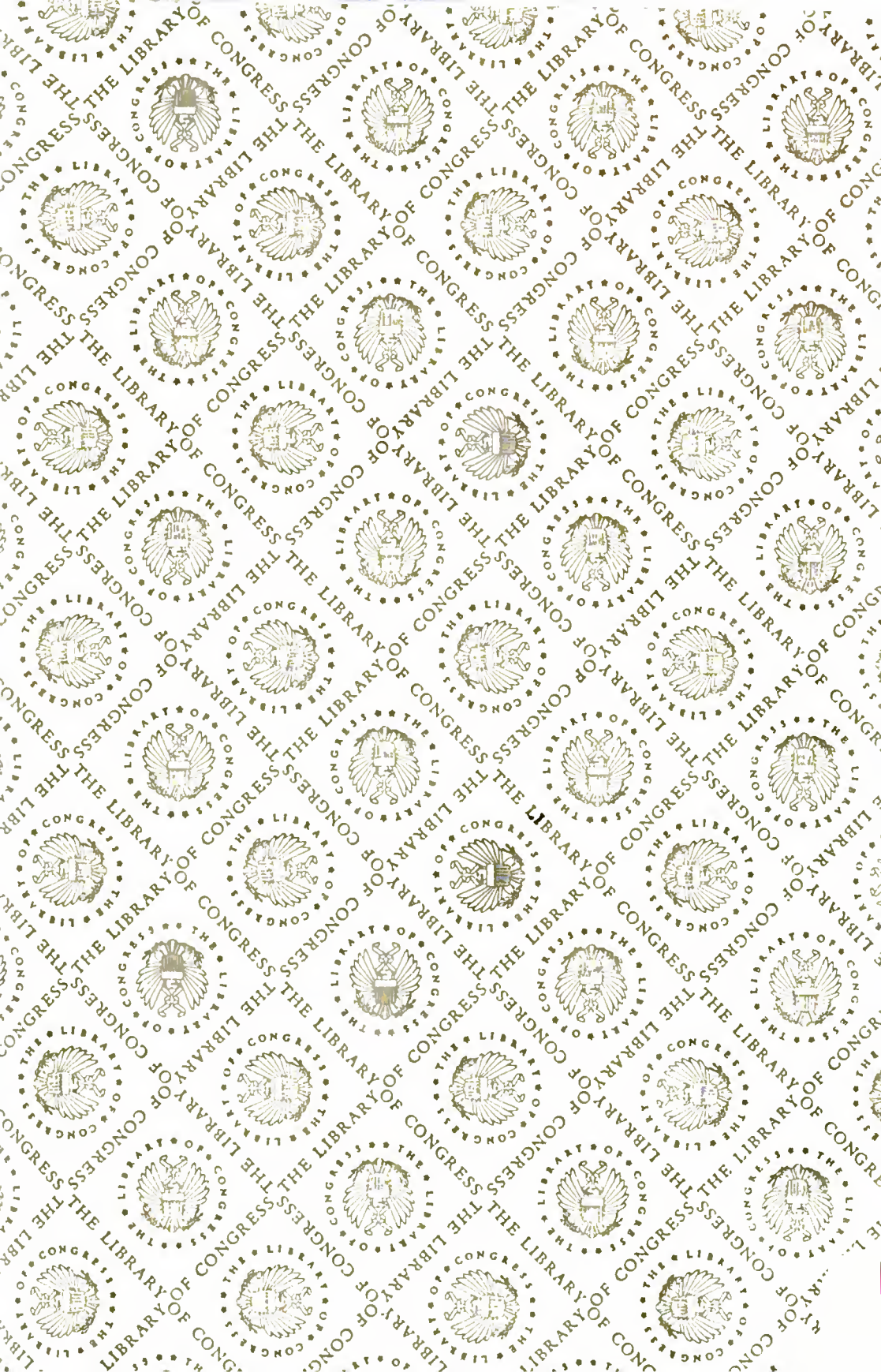

THE LIBRARY OF CONGRESS


THE LIBRARY OF CONGRESS

PRIVACY IN ELECTRONIC COMMUNICATIONS

United States

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

MARCH 26, 1998

Serial No. 132

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

59-923 WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-060029-4

COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVEN SCHIFF, New Mexico
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB INGLIS, South Carolina
BOB GOODLATTE, Virginia
STEPHEN E. BUYER, Indiana
SONNY BONO, California
ED BRYANT, Tennessee
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRIS CANNON, Utah
JAMES E. ROGAN, California
LINDSEY O. GRAHAM, South Carolina

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey

THOMAS E. MOONEY, *Chief of Staff-General Counsel*
JULIAN EPSTEIN, *Minority Staff Director*

SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
SONNY BONO, California
EDWARD A. PEASE, Indiana
CHRISTOPHER B. CANNON, Utah
BILL McCOLLUM, Florida
CHARLES T. CANADY, Florida

BARNEY FRANK, Massachusetts
JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts

MITCH GLAZIER, *Chief Counsel*
BLAINE MERRITT, *Counsel*
VINCE GARLOCK, *Counsel*
DEBBIE K. LAMAN, *Counsel*
ROBERT RABEN, *Minority Counsel*
VERONICA ELIGAN, *Staff Assistant*

CONTENTS

HEARING DATE

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

APPENDIX

PRIVACY IN ELECTRONIC COMMUNICATIONS

THURSDAY, MARCH 26, 1998

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS AND
INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee convened at 10 a.m. in Room 2237 of the Rayburn House Office Building, the Honorable Howard Coble, chairman of the subcommittee, presiding.

Present. Representatives Howard Coble, [chairman], Barney Frank, F. James Sensenbrenner, Jr., William D. Delahunt, James E. Rogan, Bob Goodlatte, and Edward A. Pease.

Also present. Mitch Glazier, Chief Counsel; Debbie Laman, Counsel; Robert Raben, Minority Counsel; and Veronica Eligan, Staff Assistant.

OPENING STATEMENT OF CHAIRMAN COBLE

Mr. COBLE. Good morning, ladies and gentlemen, and welcome to our subcommittee hearing. The subcommittee will conduct an oversight hearing on privacy in electronic communications. This hearing was suggested by the Ranking Member of this subcommittee, Mr. Frank of Massachusetts, and I am pleased to begin exploring this very important and very delicate issue.

In the technologically advanced world in which we live privacy in electronic communications is of vital importance to individuals and businesses. The ability to intercept, descramble and eavesdrop on private electronic communication over the Internet and cellular and digital communications places the privacy of individuals and businesses in jeopardy. That in turn deteriorates the incentive for individuals and businesses to engage in electronic commerce, and as a result stifles the growth of American business. It also places at risk the fundamental right of individuals to keep personal information private.

I look forward to the informative and hopefully illuminating educational hearing today.

This is an area, folks, and I'm just thinking aloud now, where it's not unreasonable for citizens to want some sort of assurance of privacy when they disclose certain private information on the Internet, and some sort of assurance that the public at large won't be able to intercept or descramble and come into possession of that information. Descrambling on the part of third party individuals and/or the government has indeed become a problem.

So having said that, I am pleased to recognize the gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Thank you, Mr. Chairman.

I don't have an opening statement, but I would associate myself with your remarks. I think this is an issue that is starting to emerge in the public consciousness, and I expect that this will be the first of a number of oversight/educational hearings that we will conduct on this particular issue.

I would ask the witnesses, and this is rather an informal hearing, to describe, if they can, those laws that are currently invoked with respect to the protection of privacy as they apply to digital, cellular and communications over the Internet. That I think would be a good start to give the members of this subcommittee a sense of what the current status is of the laws of privacy in terms of these kinds of communications.

Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

Mr. Rogan of California, do you have an opening statement?

Mr. ROGAN. Mr. Chairman, thank you.

I waive an opening statement.

Mr. COBLE. I see Mr. Frank has joined us, and I'll wait until he——

Mr. FRANK. Go ahead.

Mr. COBLE. All right. Mr. Frank can speak to us later.

Our first panel, Ambassador David Aaron has been the United States permanent representative to the Organization of Economic Cooperation and Development, OECD, since September, 1993. In addition to his responsibilities as Ambassador to the OECD, Under Secretary Aaron has been designated Special Envoy for Cryptography . His responsibility is to promote growth in international electronic commerce and robust, secure global communications in a manner that protects the public safety and the United States national security.

Next we will hear from Mr. David Medine, Associate Director for Credit Practices of the Bureau of Consumer Protection of the Federal Trade Commission. Mr. Medine is responsible for enforcing numerous Federal credit statutes, including the Equal Credit Opportunity Act, Truth in Lending Act, Fair Debt Collection Practices Act and Fair Credit Reporting Act, as well as the Federal Trade Commission Act. He has testified before Congress on numerous occasions and has worked on a number of policy issues relating to consumer protection in cyberspace.

We welcome you, Mr. Medine, and Ambassador Aaron in absentia until he gets here.

[Ambassador Aaron joins Mr. Medine at the witness table.]

Ambassador, it's good to have you with us. If you all can please confine your comments to 5 minutes. I assure you your written testimony has been and will be examined thoroughly. You will know your 5 minutes have elapsed when you see the red light illuminate.

Having said that, let me recognize Mr. Frank if he has an opening statement.

Mr. FRANK. Having come late, Mr. Chairman, I will pass on that. I appreciate your convening this hearing giving us a chance to talk about this. I would say obviously this late in this session we're not

going to be doing anything legislatively now, but I think it is important that we begin this period of consideration. There may very well need to be some legislation, and this gives us a good start. So I encourage those who have an interest who may be here listening to take advantage of our being here and to follow up on this because I do believe that by the next Congress the time will be ripe for some legislation, and this is the right way to begin to go about it.

I also would note as people read about all the contention and acrimony that besets this committee that it is nice also to have an example that we can remind people that most of the work most of the time goes forward in a very straightforward, non-partisan and non-ideological way, and we may reserve the right to yell at each other next week. But I do think we should be explicit that the differences that we have where they exist in no way hinders our ability to work together in non-ideological and non-partisan ways to do important business.

Mr. COBLE. As Mr. Frank so eloquently said on the House floor yesterday, he has yet to see a pie hurled in the direction of a Judiciary Member by a fellow Judiciary Member.

Mr. FRANK. Thank you, Mr. Chairman, and just for people from my part of the country may I point out that "pah" is spelled p-i-e. [Laughter.]

Mr. COBLE. And I thank the gentleman.

I said this earlier, but I want to credit Barney for this hearing because it was his idea. This is an area that needs attention directed to it. As Barney pointed out on the subcommittee, this issue has attracted widespread attention across the spectrum. Ideologically we have ultra-conservative and ultra-liberal advocates for this. So I look forward to hearing from you all.

Mr. Medine, if you will kick it off.

STATEMENT OF DAVID MEDINE, ASSOCIATE DIRECTOR FOR CREDIT PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. MEDINE. Thank you, Mr. Chairman and members of the committee. I appreciate the opportunity to present the Federal Trade Commission's views on the important issue of privacy on the Internet.

The Internet is an exciting new marketplace for consumers. It offers not only unprecedented ease of access to a vast array of goods and services, but also to sources of information that will enable consumers to make better informed purchasing decisions.

The Commission recognizes the importance of the development of the Internet as a viable and safe marketplace for consumers. Yet our experience and survey results teach us that in order for the online marketplace to grow sufficient privacy protections must be in place. Surveys have shown that increasing numbers of the consumers are concerned about how their personal information is used in the electronic marketplace. According to the results of a Business Week survey published just last week, consumers who are not currently using the Internet ranked concerns about privacy of their personal information and communications as the top reason they have stayed off the Internet.

The Commission's primary statutory jurisdiction in this area is the Fair Crediting Reporting Act and the Federal Trade Commission Act, which I would be happy to discuss further, not as part of my testimony, but in response to the members' concerns. We are focusing primarily in the testimony today on what the policy and self-regulatory approaches should be to Internet privacy.

The Commission's approach has been to first assess the impact of consumer protection issues for consumers online engaging in commercial transactions, to provide a public forum for the exchange of ideas and presentation of research and technology, and to encourage industry self-regulation. The Commission supports technological innovation and encourages industry self-regulation.

I want to touch on three areas of Internet privacy and privacy generally: first, look-up services; second, unsolicited e-mail and, third, online privacy generally.

First as to look-up services. In response to a growing public and Congressional concern, the Commission examined the availability of sensitive personal identifying information through computerized databases that are used to locate, identify or verify the identity of individuals. These are often referred to as individual reference services or look-up services. The Commission's study of this issue culminated in a report to Congress this past December.

The Commission found that a vast amount of information is available about consumers through these services both through proprietary networks and on the Internet. The Commission found that the look-up services provide some valuable benefits in terms of law enforcement agencies' ability to carry out their mission, parents' ability to find missing children, journalists to report the news and consumers to find lost relatives. At the same time the availability of this information poses risks to consumers' privacy and financial interests, including the possibility of increased incident of identity theft.

Fourteen companies, a substantial majority of the individual reference service industry, as well as the three major credit bureaus, agreed to abide by what are called the IRSG principles, a set of principles that address the availability of information obtained through these services. These principles primarily address access to individual information obtained from non-public sources contained in these databases.

It's noteworthy that the IRSG principles prohibit distribution to the general public over the Internet or otherwise of certain non-public individual, including Social Security number, mother's maiden name and date of birth.

These principles show particular promise because of their degree of specificity, their inclusion of a compliance assurance mechanism and the likelihood they will influence virtually the entire individual services industry.

The Commission concluded that these principles addressed many of the public concerns about these databases and suggested that these principles should be given a chance to operate before any legislation was enacted in this area.

Turning to unsolicited e-mail, the Commission has gathered a considerable body of information about the growing problem of unsolicited commercial e-mail.

Three initiatives have resulted from this effort.

One is we have encouraged a cross-section of interested parties, including Internet service providers, online firms, senders of unsolicited e-mail and privacy advocates to form a working group, which they have done under the auspices of the Center for Democracy and Technology. They are expected to issue a report outlining some proposed solutions to this problem. Second, the Commission using its existing statutory authority has brought a number of enforcement actions in this area. And, third, we've launched an educational campaign.

If I could just have an additional minute or two on online privacy generally.

Mr. COBLE. Without objection.

Mr. MEDINE. The Commission has focused extensively on the collection of information about consumers online and through its public workshops has encouraged and facilitated self-regulatory efforts. This month we are surveying 1,200 web sites to assess whether they are posting privacy policies, giving consumers choice over use of their information and giving access, as well, to that information. We will be issuing a report to Congress in June reporting on the results of that as well as assessing industry self-regulatory guidelines.

We believe the report we submit to Congress will shed light on how much progress has been made in self-regulation and in achieving effective online protection for consumers, and if progress is inadequate in this area, appropriate alternatives may need to be explored.

Thank you for the opportunity to discuss these timely issues.

[The prepared statement of David Medine follows:]

PREPARED STATEMENT OF DAVID MEDINE, ASSOCIATE DIRECTOR FOR CREDIT PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman and members of the House Judiciary Committee: I am David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of privacy on the Internet.[1]

I. INTRODUCTION

A. Internet Privacy

The Internet is an exciting new marketplace for consumers. It offers not only easy access to a vast array of goods and services, but also to rich sources of information that enable consumers to make better-informed purchasing decisions.

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada.[2] Of those people, 73% reported that they had shopped for product information on the World Wide Web ("the Web"), the interactive graphics portion of the Internet.[3] By December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million, and 10 million had

[1] My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any one Commissioner.

[2] CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old) (reported at <http://www.commerce.net/work/pilot/nielsen—96/press/97.html>) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS™)*: Second Quarter 1997 Study (Sept. 4, 1997) (reported at <http://www.intelliquest.com/about/release32.htm>).

[3] *CommerceNet/Nielsen Demographic Study*, Spring '97.

actually purchased a product or service online.[4] Further, analysts estimate that Internet advertising—which totaled approximately $301 million in 1996—will swell to $4.35 billion by the year 2000.[5]

These figures suggest rapid growth of the online marketplace, but there are also indicators that consumers are wary of participating in it. Surveys have shown that increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace. This research indicates that consumers have less confidence in how online service providers and online merchants handle personal information than they have in how traditionally off-line institutions, such as hospitals and banks, handle such information.[6] In fact, a substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are.[7] According to the results of a *Business Week* survey released earlier this month, consumers not currently using the Internet ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet.[8] These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until sufficient consumer privacy protections are implemented in the online marketplace.

B. The FTC's Role

The mission of the FTC is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission undertakes this mission by enforcing the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[9] The Commission's responsibilities are far-reaching. With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy.[10] Commerce on the Internet falls within the scope of this statutory mandate.

C. The FTC's Approach to Online Privacy

The Commission is taking a proactive approach to online privacy issues impacting consumers by: (1) identifying potential consumer protection issues related to online marketing and commercial transactions; (2) providing a public forum for the exchange of ideas and presentation of research and technology; and (3) encouraging self-regulation.

The Commission's first public workshop on privacy was held in April 1995. In a series of hearings held in October and November 1995, the FTC examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and

---

[4] CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997) (reported at <http://www.commerce.net/news/press/121197.html>) [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. *See also* Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (reported at <http://www.yankelovich, com/pr/970327.HTM>) (finding that 23% of users ordered and paid for a product over the Internet, *i.e.*, "transacted" business online).

[5] Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (reported at <http://www.jup.com/digest/08229/advert.shtml>) (figure includes directory listings and classified advertisements).

[6] *Commerce, Communications, and Privacy Online, A National Survey of Computer Users*, by Louis Harris & Associates and Dr. Alan F. Westin (1997) (hereinafter referred to as "Westin Survey") at ix.

[7] *Id.* at 20–21.

[8] "Business Week/Harris Poll: Online Insecurity," *Business Week*, March 16, 1998.

[9] 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty additional statutes, *e.g.*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[10] Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. A summary of the workshop testimony was published by the Commission in a December 1996 staff report entitled *Consumer Privacy on the Global Information Infrastructure*. The agency held a four-day workshop in June 1997 to explore issues raised by computerized databases that contain consumers' personal identifying information (also known as "individual reference services" or "look-up" services). This workshop also explored issues relating to unsolicited commercial e-mail, online privacy, and children's online privacy.

These FTC efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various consumer privacy concerns in the electronic marketplace.[11] In addition, FTC staff has written opinion letters delineating what types of practices in this area might violate the Federal Trade Commission Act.[12]

II. FOCUS OF FTC PRIVACY ACTIVITIES

Following the June 1997 workshop, the Commission focused on a number of key privacy issues impacting consumers. These issues were discussed in a July 31, 1997, letter (Attachment A) responding to a joint request from Chairman John McCain and Chairman Tom Bliley for a brief report on the Commission's findings from the workshop. The Commission's letter summarized its work and provided a plan to address concerns raised by the following issues: (1) computerized databases containing consumers' personal identifying information, *i.e.*, individual reference services or look-up services; (2) unsolicited commercial e-mail; (3) online information collection; and (4) children's privacy in the online environment. I will address each of these issues today. In addition, as set forth in the July 31 letter, the Commission intends to issue a report to Congress in June 1998 that will focus on the Commission's efforts to monitor and assess the status of self-regulatory efforts by industry members involved in the online collection and dissemination of consumer information.

A. Individual Reference Services

In response to growing public and Congressional concern, the Commission examined the availability of sensitive personal identifying information through computerized database services that are used to locate, identify, or verify the identity of individuals, often referred to as individual reference services or look-up services. The Commission's study of look-up services culminated in a report to Congress in December 1997. The report summarized what the Commission had learned about the individual reference services industry; examined the benefits, risks, and potential controls associated with these services; assessed the viability of an industry self-regulatory proposal; and concluded with recommendations that address concerns left unresolved by the proposal.[13]

The Commission found that a vast amount of information about consumers is available to customers of individual reference services through the services' proprietary computer networks and increasingly over the Internet. Gleaned from various public and proprietary sources, information available through the services ranges from purely identifying information, *e.g.*, name and phone number, to much more extensive data, *e.g.*, driving records, criminal and civil court records, property records, and licensing records.[14] The Commission also learned that convenient access to this type of information confers a myriad of benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, parents to find missing children, journalists to report the news,

---

[11] *E.g.*, FTC Report to Congress: *Individual Reference Services*, December 1997; FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996. In addition, the Commission presented testimony on September 18, 1997, on the Implications of Emerging Electronic Payment Systems on Individual Privacy before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services.

[12] *E.g.*, Letter from Bureau of Consumer Protection Director to Center for Media Education, July 15, 1997.

[13] FTC Report to Congress: *Individual Reference Services*, December 1997.

[14] *Id.* at 4–5.

and consumers to find lost relatives.[15] At the same time, the increasing availability of this information poses various risks of harm to consumers' privacy and financial interests, including the possibility of increasing the incidence of identity theft.[16]

At the June 1997 workshop, a group of industry members (the "Individual Reference Services Group" or "IRSG") announced its intent to address concerns associated with its industry through self-regulation. Commission staff worked with this group to encourage it to adopt an effective self-regulatory program. In December 1997, 14 companies, a substantial majority of the individual reference service industry, agreed to abide by the "IRSG Principles," a set of principles that addresses the availability of information obtained through individual reference services.

The IRSG Principles restrict access to certain information obtained from "non-public" sources contained in each signatory's database. This non-public information includes what is called "credit header" information, which is that portion of a credit report purchased from a credit reporting agency that contains an individual's name, address, aliases, Social Security number, current and prior addresses and telephone number.[17] The restrictions vary according to the category of customer. Customers that have less restricted access to non-public information are subject to greater controls. It is noteworthy that the IRSG Principles prohibit distribution to the general public—over the Internet or otherwise—of certain non-public information, including Social Security number, mother's maiden name, and date of birth. In addition, consumers will be able to access the non-public information maintained about them in these services and to prevent the sharing (*i.e.*, "opt out") of the non-public information distributed to the general public.[18]

The IRSG Principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry. First, signatories must undergo an annual compliance review by a professional third party such as an accounting firm, the results of which will be made public. Public examination of the results of compliance reviews and the possibility of liability under the FTC Act and similar state statutes should create an incentive for compliance by signatories. Second, signatories that are information suppliers (*e.g.*, the three national credit reporting agencies) are prohibited from selling information to entities whose practices are inconsistent with the Principles. Therefore, non-signatories whose practices are inconsistent with the Principles likely will be unable to obtain non-public information easily for redissemination through their services. Thus, the IRSG Principles should substantially lessen the risk that information held by these services will be misused, and they should address consumers' concerns about the privacy of their non-public information.[19]

The Commission concluded that the IRSG Principles address many of the concerns associated with the increased availability of non-public information through individual reference services while preserving important benefits conferred by this industry. However, important issues related to individual reference services remain. For example, the IRSG Principles do not give consumers access to the "public information" (*e.g.*, real estate, motor vehicle, and court records) maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services. IRSG members have agreed to revisit this issue by June 1999, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission has urged the IRSG to conduct an analysis to determine whether the frequency of inaccuracies and the harm associated with them are such that consumer access to public record information or other safeguards are in fact unnecessary.[20]

In its report to Congress, the Commission also encouraged public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. Finally, the Commission has acknowledged and encouraged the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG to educate the public about information privacy issues.[21]

---

[15] *Id.* at 9–11.
[16] *Id.* at 13–16.
[17] *Id.* at 5–6 and n. 42. Non-public information on an individual's financial status, employment background, credit history, and medical records can be found in a credit report, but the dissemination of that information by a credit reporting agency is strictly regulated under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681u (1997).
[18] *Id.* at 25–28.
[19] *Id.* at 28–30.
[20] *Id.* at 31–32.
[21] *Id.* at 32–33.

B. Unsolicited Commercial E-mail

At the 1997 Workshop, the Commission also gathered a considerable body of information concerning the problem of unsolicited commercial e-mail ("UCE"). Three UCE-related initiatives grew out of that workshop. First, a cross-section of interested parties, including Internet service providers, online firms, senders of UCE, and privacy advocates, formed a working group to develop a self-regulatory solution to the problems associated with UCE. This group, which has been led by the Center for Democracy and Technology, a non-profit, public interest organization involved in new technology issues, is expected to issue a report outlining proposed solutions. Second, the Commission brought enforcement actions against scam artists who make allegedly fraudulent solicitations via UCE,[22] and continues to investigate other possible frauds committed through UCE. Third, the Commission has launched an educational campaign. Staff have produced educational materials warning consumers to be suspicious of the solicitations they receive in UCE and are distributing them through channels designed to reach those who are likely to use e-mail. Staff also monitored thousands of UCE messages, identified those which appeared facially deceptive, and sent letters to over one thousand senders of these UCE messages, advising them of the legal requirements applying to their activities.

C. Online Information Collection Practices

Many consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.[23] During the Commission's first privacy workshop, a consensus emerged among workshop participants regarding four important considerations that would assist in protecting online privacy. These considerations include: *notice* concerning Web sites' information practices, *i.e.*, how commercial Web sites will use personal information they collect from consumers; *choice* in how Web sites will use consumers' personal information; *access* to consumers' own information collected, maintained, or used by Web sites; and *security* of consumers' personal information maintained by Web sites from improper or unauthorized use by third parties.[24]

1. Commitment to Self-Regulation

The Commission has also learned that members of the online industry are aware of the need to address consumers' concerns. Throughout the series of Commission workshops on these issues, the online industry has asserted that self-regulation is the most efficient and effective means of creating online privacy protections. Industry groups have demonstrated varying approaches to protecting online consumer privacy. As of June 1997, certain key trade associations had developed policies and procedures to protect online privacy. Others were in the initial stages of policy formation, and still others remained uncertain as to whether industry-wide policies, as opposed to individual company efforts, would be necessary. Trade association representatives committed to develop privacy policies as guidance for their members and to encourage their members to post their own information practices on their Web sites. In addition, a non-profit group called TRUSTe launched a proprietary system requiring disclosure of member Web sites' basic information practices and third-party auditing of those practices, but the system had not yet been widely implemented.[25] Its efficacy will depend upon widespread industry participation.[26]

The Commission has also learned of promising efforts to create interactive technology that permits consumers to automate their preferences, and Web sites to communicate their practices, regarding the collection and use of personal information online. At the time of the 1997 Workshop, these technological tools, which potentially could provide adequate privacy protection, were still in the initial stages of development.[27]

---

[22] *See FTC* v. *Maher*, Case No. WMN–98–495 (D. Md. filed Feb. 19, 1998) (unsolicited commercial e-mail promoting allegedly bogus business opportunity); *FTC* v. *Cooley*, CIV–98–0373 PHX–RGS (D. Ariz. filed Mar. 4, 1998) (unsolicited commercial e-mail promoting allegedly fraudulent credit repair services).

[23] *Privacy & American Business Report*, Vol. 4, No. 3 (1997) (reporting on Louis Harris Associates and Alan F. Westin's *National Survey of Computer Users*).

[24] FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996.

[25] *See* Transcript from FTC Public Workshop on Consumer Information Privacy, June 11, 1997 at 108–112.

[26] As noted on page 17 *infra*, the Commission has recently requested information practice guidelines and principles from trade associations and industry groups to determine the current status of these efforts.

[27] *See* Transcript from FTC Workshop on Consumer Information Privacy, June 13, 1997 at 81–82.

2. Online Information Collection from and about Children

The collection of information from and about children who use the Internet deserves special attention. Internet usage by children is growing: a 1997 survey indicates that approximately 9.8 million children (under age 18) go online, which is a five-fold increase from 1995.[28] Children use the Internet for a variety of activities including homework or informal learning, playing games, browsing or for e-mail/chat rooms.[29] These young people are not shopping or banking online, but parents still have serious concerns about the online collection and use of personal information from children. A 1997 survey indicates that 97 percent of parents whose children use the Internet believe Web sites should not sell or rent personal information on children; 80 percent object to a Web site requesting a child's name and address when the child registers, even if such information is used only internally.[30]

Several workshop participants voiced concern at the 1997 Workshop about online activities that enable children to post or disclose their names, street addresses, or e-mail addresses in areas accessible to the public, such as chat rooms, bulletin boards, and electronic pen pal programs, creating a serious risk that the information may fall into the wrong hands.[31] For example, anecdotal evidence indicates that many children surfing the Internet claim to have experienced problems, such as attempted password theft and inappropriate advances by adults in children's chat rooms.[32] Further, the FBI and Justice Department's "Innocent Images" investigation reveals that online services and bulletin boards are rapidly becoming the most prevalent sources used by predators to identify and contact children.[33]

Industry guidelines on the collection and use of children's information were presented by the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus and by the Direct Marketing Association, among others.[34] All of the guidelines call for some form of notice and some degree of parental choice over the disclosure of personal information about children to third parties. The guidelines, however, do not always make clear what specific steps would satisfy these obligations or take into account that children may be online without parental supervision.

Overall, there was strong support at the 1997 Workshop for development of technological tools, such as filtering or browser software, to protect children's privacy. Yet, important limitations were identified, such as the ability of computer-savvy children to defeat technological protections and the fact that their widespread implementation and use may be over a year away.[35] These technologies are only now being applied to protecting privacy, and their effectiveness will depend on their widespread adoption by industry and parents.

Finally, the information presented at the 1997 Workshop demonstrated the need to educate parents about privacy issues concerning their children's use of the Internet and the need for parents to establish clear rules for children on providing information to Web sites. Commission staff is developing additional educational materials for parents and children regarding privacy protections for children online and, most importantly, looking for ways to work with affected industries, consumer groups, and educators to develop educational initiatives.[36]

3. Encouraging Self-Regulation

The Commission has encouraged industry to address consumer concerns through self-regulation. In the Commission's view, self-regulation in the first instance generally is more prompt, flexible, and effective than government regulation. Further, self-regulation can bring the accumulated judgment and experience of industry to bear on issues that may be difficult for the government to define with bright-line rules. Industry and consumers are well-situated to know what is needed and where

---

[28] *Interactive Consumers Research Report*, Vol. 4, No. 5 at 1, May 1997 (discussing results of FIND/SVP's 1997 American Internet User Survey).

[29] *Id.*

[30] *See* Transcript from FTC Public Workshop on Consumer Information Privacy, June 12, 1997, at 156 (citing Westin Survey at 74).

[31] *Id.* at 230.

[32] *Id.* at 192–93.

[33] *Id.*

[34] *Id.* at 132–78 (June 13, 1997).

[35] *Id.* at 25–26.

[36] In response to a petition from the Center for Media Education concerning the information collection practices of "KidsCom," a web site directed to children, the Commission staff issued an opinion letter addressing potential Section 5 violations involved in the collection of personally-identifiable information directly from young children. Letter from Bureau Director Jodie Bernstein to Center for Media Education, July 15, 1997.

immediate concerns lie. The IRSG Principles provide one promising model for self-regulation.

Commission staff has recently issued some guidance that should strengthen self-regulatory efforts to protect consumers' privacy both online and off-line. The Commission staff recently responded to a request from the Direct Marketing Association ("DMA") for an advisory opinion concerning whether the antitrust laws would permit it to require three things of its members: (1) to use the DMA's Mail Preference and Telephone Preference Services to honor consumers' requests to not be contacted by direct marketers; (2) to disclose to consumers how members sell or otherwise transfer personal information about those consumers to others; and (3) to honor consumers' requests that the members not sell or transfer their personal information. FTC Bureau of Competition staff advised the DMA of its conclusion that these requirements, as the DMA described them, would not harm competition or violate the FTC Act.[37]

4. Monitoring Self-Regulation

The Commission continues to monitor the online collection and use of information from consumers, including children. Last October, Commission staff conducted a "Kids Privacy Surf Day," designed as a "quick snapshot"—not a comprehensive survey—of children's Web sites' privacy practices. Staff found that more than 80 percent of the over 100 sites surveyed were collecting personal identifying information from children, most without seeking parental permission or allowing parents to control the collection and use of the information. Commission staff sent the surveyed Web sites e-mail messages notifying them of potential law violations in connection with their information collection practices.

This month, the Commission is conducting a survey of commercial Web sites, including sites directed to children, to determine the extent to which they are disclosing their information practices and offering consumers choice regarding the online collection and use of their personal information. The survey covers approximately 1200 Web sites: 100 of the most frequently visited Web sites; roughly 900 sites drawn from a database of commercial Web sites maintained by Dun & Bradstreet, including subsamples representing the retail, health, and financial sectors; and roughly 200 children's sites drawn from Yahooligans' online directory of sites of interest to children. In particular, the Commission is looking at whether sites display privacy policies or discrete statements about their information practices and whether such disclosures (1) include notice to consumers as to whether their information will be transferred to third parties; (2) provide consumers with choice over the use of their information; (3) allow consumers to access the information that is maintained about them; and (4) inform consumers that security precautions will be taken to protect their information after it has been transferred. Further, the Commission is assessing whether the policies are easy to find. As to sites directed to children, the Commission is also determining whether individual sites allow parents to have control over the collection, disclosure, and use of their children's information.

III. REPORT TO CONGRESS: ASSESSING STAFF'S FINDINGS

As mentioned above, the Commission's upcoming report to Congress will focus on the effectiveness of self-regulation as a means of protecting consumer privacy online. The Commission will summarize and assess its findings from this month's comprehensive survey of commercial Web sites. The report will also include the Commission's analysis of existing industry guidelines and principles on the online collection and use of consumers' personal information. Toward that end, the Commission issued a *Federal Register* notice on March 5, 1998, requesting that interested trade associations and industry groups submit copies of their information practice guidelines and principles for inclusion in the Commission's report.

IV. CONCLUSION

The Commission recognizes the importance of the development of the Internet as a viable and safe marketplace for consumers. In order for the online marketplace to grow, sufficient privacy protections must be in place. The Commission supports technological innovation and also encourages industry self-regulation so long as self-regulation proves meaningful and effective. The upcoming June report describing the results of the staff's Web survey will shed light on how much progress self-regulation has made in achieving effective online privacy protection for consumers. If such progress is inadequate, appropriate alternatives may need to be explored.

[37] Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997.

ATTACHMENT A

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION,
Washington, DC, July 31, 1997.

Hon. JOHN MCCAIN, *Chairman,*
Committee on Commerce, Science and Transportation,
United States Senate, Washington, DC.

DEAR MR. CHAIRMAN: This letter responds to your letter dated July 30, 1997 requesting that the Commission provide Congress with a preliminary assessment of the Public Workshop on Consumer Privacy held on June 10–13, 1997. The Workshop addressed four major topics: computerized databases containing identifying information about consumers; unsolicited commercial e-mail; consumers' online privacy; and children's privacy in the online environment. The Workshop presentations and the extensive written commentary submitted in connection with the Workshop form a rich public record with which to examine these subjects. We welcome this opportunity to provide our preliminary findings from the Workshop and to outline some of the steps the Commission intends to undertake in the next twelve months to address consumer privacy issues.[1]

Computerized Databases

In light of widespread concern and Congressional interest, the Commission previously agreed to conduct a study of the collection, compilation, sale, and use of computerized databases that contain what consumers may perceive to be sensitive identifying information, often referred to as "look-up services," "locators," or "individual reference services." The Workshop, as well as the comments which have been and continue to be filed, will aid us in completing this ongoing study. At the Workshop, database operators, information vendors and other participants identified the types and sources of information contained in their databases. A wide variety of personal information, including social security numbers, dates of birth, unlisted phone numbers, prior addresses, and the names and ages of household members, is being collected and stored in databases. In some cases, this data is made instantly available to anyone with access to the Internet.

Workshop participants discussed the benefits and risks associated with look-up services. Database users demonstrated the crucial role that these databases play in furthering important objectives, such as tracking down criminals, preventing fraud, finding witnesses, preparing news reports, and locating missing children. Privacy and consumer advocates expressed concerns about the privacy implications of the databases and warned of potential harm that could result from inaccurate or insecure data, as well as from the misuse of the data for criminal ends, including identity theft.

We are encouraged that the industry has stepped forward to address the serious privacy concerns raised by these databases. Key industry members came together and offered a preliminary self-regulatory proposal to limit the availability of sensitive information, to ensure the accuracy and security of this information, and to educate consumers about their practices.

Workshop participants and Commission staff have identified a number of key issues to address in the Commission's study of computerized databases. These issues include: preventing misuse of personal information; providing consumers with sufficient access to their own information to correct inaccuracies; avoiding undue chilling of the free flow of information for legitimate purposes; assessing the effectiveness of self-regulatory guidelines and enforcement mechanisms; and examining the extent to which government action, if any, may be needed.

The Commission anticipates submitting a report on the database study to the Congress by the close of 1997. We plan to continue our dialogue with industry members to help improve and broaden the reach of their self-regulatory effort.

Unsolicited Commercial E-mail

Survey research presented at the Workshop demonstrates that unsolicited commercial e-mail is strongly disfavored by almost all consumers who receive it. It imposes considerable costs (in time and money) on individual recipients and their online or Internet service providers, and the large volume of bulk e-mail solicitations burdens the infrastructure of the Internet itself. These costs are likely to escalate

[1] The public record for the unsolicited commercial e-mail and online privacy sessions of the Workshop closed on July 14, 1997. The public record for the session on computerized databases remains open. The transcript of the Workshop and all commentary submitted has been posted on the Commission's Web page (www.ftc.gov).

as e-mail solicitations become interactive and incorporate video and audio messages that further consume the Internet's capacity and use more space on recipients' computers. Furthermore, an increasing segment of unsolicited commercial e-mail involves seemingly fraudulent offering of products or services, such as get-rich-quick schemes that we commonly see in our telemarketing fraud program. In addition, in what appears to be unique to this form of direct marketing, unsolicited e-mail often involves the use of false return addresses and forged header information, practices which may also be deceptive within the meaning of Section 5 of the Federal Trade Commission Act.

We recognize, however, that interactive technology provides a unique and potentially lucrative marketing medium. It is an extremely inexpensive way for small businesses and entrepreneurs to reach a broad audience. E-mail also holds out the promise of one-to-one marketing of bona fide products and services to consumers who truly wish to receive solicitations in this manner. Workshop participants discussed various ways to identify those consumers. For the most part, industry groups favor providing consumers with the opportunity to have their e-mail addresses removed from lists created for the purpose of sending unsolicited commercial e-mail. Another approach which some individual online marketers have found successful is the use of lists which include only individuals who have affirmatively asked to receive e-mail solicitations.

The Workshop provided both proponents and opponents of the practice of sending unsolicited commercial e-mail with the opportunity to come to one table. We are encouraged that a disparate group, including senders of unsolicited commercial e-mail, technology experts, and privacy advocates, has committed to develop a voluntary response to consumer and industry concerns and to report back to the Commission in 6 months. Staff will monitor this self-regulatory effort. In addition, staff will continue to monitor unsolicited commercial e-mail for possible violations of Section 5 of the Federal Trade Commission Act, and the Commission will bring enforcement actions, as appropriate, against senders who engage in fraudulent or deceptive practices.

Consumer Online Privacy

The Workshop demonstrated that many consumers care deeply about the security and confidentiality of their personal information in the online environment. Consumer survey research presented at the Workshop indicates they are looking for greater protections, preferably from voluntary efforts by industry, but if necessary from government. Currently a handful of commercial sites on the World Wide Web disclose how they collect and use consumer information online and offer consumers an opportunity to exercise choice as to whether and how their information should be used. Members of the online industry are aware of the need to address consumers' concerns, and have begun to respond with self-regulatory measures.

We are delighted with the high level of interest in our efforts shown by the industry leaders who submitted commentary and chose to participate in the Workshop. Industry groups demonstrated varying approaches to protecting online privacy. Some key trade associations have well-developed policies and procedures; others are in the initial stages of policy formation; still others remain uncertain as to whether industry-wide policies, as opposed to individual company efforts, are necessary. Even when a Web site has a policy, its effectiveness depends on whether the policy is easily communicated to consumers.

The McGraw-Hill Companies, a Workshop participant whose corporate divisions sponsor sixty Web sites, is implementing a privacy policy that is one model for companies committed to protecting consumer privacy online. This policy requires: (1) that consumers be notified of the collection and intended uses of their personally identifiable information; (2) that consumers be offered the opportunity to refuse permission for distribution of their personally identifiable information to third parties; (3) that security measures be implemented to protect the integrity and privacy of this information; (4) that consumers have access to this information and a mechanism to correct it; and (5) that measures be implemented to ensure that only authorized third parties use this information, and only for authorized purposes. The policy prohibits the distribution outside the company of "sensitive" personally-identifiable information, including medical and financial data, as well as most information about children. Consumers will also be given the ability to prevent this sensitive information from being shared even among the company's subdivisions.

The Workshop also highlighted a variety of other self-regulatory endeavors. A proprietary system requiring disclosure of member Web sites' basic information practices and third-party auditing of those practices has been launched, but has not yet been widely implemented. Its efficacy as a privacy protection will depend upon widespread industry participation. Particularly promising are efforts to create interactive

technology that permits consumers to automate their preferences, and Web sites to communicate their practices, regarding the collection and use of personal information online. These technological tools, which may well provide adequate privacy protection, are in the initial stages of development. They will play a critical role in any comprehensive self-regulatory solution to online privacy concerns.

Self-regulatory approaches and emerging technological tools will be effective in protecting online privacy only to the extent that they are widely adopted by Web sites and, in the cast of technology, are readily available to consumers and easy to use. Consumer and business education projects will be critical to the success of these efforts, and the Commission will assist industry and consumer groups in those endeavors.

Commission staff will monitor the World Wide Web, just as it monitors national advertising, to determine the extent to which commercial Web sites are disclosing their information practices and offering consumers choice regarding the collection and use of their personal information online. We will report our findings to Congress on or before June 1, 1998. Our recommendations, if any, will take into account whether the initial efforts demonstrated at the Workshop are translated into broader industry progress toward effective self-regulation.[2]

Children's Online Privacy

The final focus of the Workshop was the special problems posed by the collection of information from children who use the Internet. The presentations provided valuable information regarding (1) parents' attitudes and perceptions on online information collection from children; (2) Web sites' information collection practices and policies; (3) industry initiatives; and (4) possible technological responses to address children's privacy concerns.

Consumer survey data presented at the Workshop showed that consumers generally, and particularly parents, are extremely concerned about the collection of personally-identifiable information from children. Parents are virtually unanimous (97%) in their belief that Web sites should not collect personal information from children, and sell or rent that information to others. Similarly, 72% of parents object to a Web site's asking children to provide their names and addresses when they register, even when the site uses this information only within the company; 64% object to a Web site's asking children to provide their e-mail names to gather statistics on how many children visit the site and what they do there. In addition, anecdotal evidence indicates that as many as one third of children surfing the Internet claim to have experienced problems, such as attempted password theft and inappropriate advances by adults in children's chat rooms. Information presented at the Workshop indicates that numerous Web sites are collecting a variety of personal information from children without providing effective notice to parents, although there was less information about how and in what form the data is used once collected.

Special concern was voiced at the Workshop about online activities that enable children to post or disclose their names, street addresses, or e-mail addresses in areas accessible to the public, such as chat rooms, bulletin boards, and electronic pen pal programs, creating a serious risk that the information may fall into the wrong hands. In fact, the FBI and Justice Department's "Innocent Images" investigation reveals that online services or bulletin boards are rapidly becoming one of the most prevalent sources used by predators to identify and contact children.

At the Workshop, participating industry groups stated their commitment to effective self-regulation. Industry guidelines on the collection and use of children's information were presented by the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus and by the Direct Marketing Association, among others. These guides, however, have only recently been released, and industry is just beginning its efforts to educate Web site operators and seek compliance. In general, the recent issuance of industry guidelines in the children's area demonstrates the industry's commitment to addressing this problem. Nonetheless, there were concerns about the sufficiency of the guidelines. While all of the guidelines call for some form of notice and some degree of choice over the disclosure of personal information about children to third parties, the guidelines do not make clear what specific steps would satisfy these obligations. The extent and speed of industry compliance with the new guidelines will be important to evaluating whether action by government is needed.

Overall, there was strong support at the Workshop for development of technological tools to protect children's privacy. The testimony also identified important

[2] We hope to find by March 1, 1998, that a substantial majority of commercial Web sites are clearly posting their information practices and privacy policies. Commission staff will also be looking to see whether Web sites are honoring consumers' privacy preferences.

limitations on the ability of current products to protect children's privacy. First, computer-savvy children can easily defeat them.[3] Second, although, 85% of parents say they would use filters if they were inexpensive and easy to operate, only 25% of parents said they were currently using them.[4] Third, while newer, interactive technologies to enhance children's online privacy were also demonstrated, their widespread implementation is at least one or more years away. For example, a new technical standard is being developed that would allow parents to set privacy preferences for their children automatically. In addition, other technologies such as digital certificates and biometric technology were presented as possible means of obtaining verifiable parental consent in the future. These technologies are only now being applied to protecting privacy, and their effectiveness will depend on their widespread adoption by industry and parents.

The staff is taking a number of steps to address the important issues raised by the online collection of information from and about children. First, in response to a petition to the Commission from the Center for Media Education (CME), the staff of the Bureau of Consumer Protection recently issued the attached letter denying the petition. The letter also provides the industry with initial staff guidance with respect to online information practices that could be deemed deceptive or unfair under Section 5 of the FTC Act.

Second, having provided initial staff guidance in the CME letter, the staff will continue to review the online collection and use of information from children by commercial Web sites and will recommend that the Commission initiate enforcement actions where appropriate. We believe that carefully selected enforcement actions will help support effective industry self-regulation.

Third, Commission staff will continue to support self-regulatory efforts, as well as technological responses to this issue. We will include our assessment of the industry's self-regulatory efforts in our June 1998 report to Congress. In preparing this report, we will assess the percentage of sites providing notice to parents, whether the notice meets the criteria set forth in the staff's response letter to CME, what information is being collected from children, and how Web sites are using this information.

Fourth, the staff will continue to pursue a dialogue with industry about the desirability of FTC guidelines in the area of children's online privacy. The Workshop revealed uncertainty in the business community about what constitutes an unfair or deceptive practice in the context of online information collection from children. The CME letter and any future enforcement actions may provide adequate guidance, but we will also continue to explore the possibility of guides that would further clarify what information practices would constitute an unfair or deceptive practice under Section 5.

Finally, the information presented at the Workshop demonstrated the need to educate parents about privacy issues concerning their children's use of the Internet and the need for parents to establish clear rules for children on information disclosure to Web sites.[5] Commission staff will develop additional educational materials for parents and children regarding privacy protections for children online and, most importantly, look for ways to work with affected industries, consumer groups, and educators to develop educational initiatives.

Conclusion

The Workshop proved to be an invaluable source of information to assist our consumer privacy efforts. In sum, these efforts include the following steps. We expect to report to Congress on the database study by the end of 1997. We plan to monitor industry's self-regulatory efforts in connection with unsolicited commercial e-mail and to bring enforcement actions, as appropriate, against senders whose practices violate the Federal Trade Commission Act. We also will monitor the information practices of commercial sites on the World Wide Web, and we will report our findings on the effectiveness of self-regulation to Congress by June 1, 1998. With regard to children's online privacy, we will monitor industry's implementation of its guide-

[3] Some of the filters do not screen for disguised names—even simply separating a first and last name with a period can bypass a filter programmed to block the first and last name of a child. In addition, none of the filters reportedly guard against a child giving up information via check boxes, multiple choice menus, or as an e-mail attachment.

[4] For this reason, it appears that these filters may be widely used only if they are incorporated into Web browsers, rather than left to individual parents to obtain.

[5] For example, one industry effort offers the following online safety rule: "I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission." *Child Safety on the Information Highway*, National Center for Missing and Exploited Children and the Interactive Services Association (1994).

lines, review online information collection practices by commercial Web sites, take enforcement action, where appropriate, and report our findings to Congress. We will continue to educate consumers and industry about information privacy issues in all these areas.

We appreciate your continued interest in, and support of, our work in this area.

By direction of the Commission.

DONALD S. CLARK, *Secretary.*

ATTACHMENT B

Madam Chairman and members of the Committee: I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of fraud on the Internet.[1]

Introduction

The Commission pursues its mission of promoting the efficient functioning of the marketplace by seeking to protect consumers from unfair or deceptive acts or practices and to promote vigorous competition. As you know, the Commission's responsibilities are far-reaching. Its primary legislative mandate is to enforce the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[2] With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy;[3] commerce on the Internet falls within the broad sweep of this statutory mandate.

The advent of the Internet—with its new methods of communicating through web sites, electronic mail, news groups, chat rooms, electronic bulletin boards, and commercial on-line services—is an historical development much like the introduction of television or, a few generations earlier, the telephone. Like these earlier technologies, the Internet presents consumers with an exciting new means for them to purchase both innovative and traditional goods and services faster and at lower prices, to communicate more effectively, and to tap into rich sources of information that were previously difficult to access and that now can be used to make better-informed purchasing decisions.

The Internet's promise of substantial consumer benefits is, however, coupled with the potential for fraud and deception. Fraud is opportunistic, and fraud operators are always among the first to appreciate the potential of a new technology. This phenomenon was illustrated by the advent, flourishing, and near-demise of pay-per-call (900-number) technology as a commercial medium during the last decade. 900-number technology was the first interactive technology—and still is the only interactive technology offering nearly universal access because all that is needed is a telephone. This technology has huge potential as an alternative payment system, since every telephone could serve as a payment terminal, and no credit cards, debit cards, or checks are needed. In 1991, there were $6 billion in pay-per-call transactions. But fraud operators moved in to exploit the technology, and the industry was slow to respond to this challenge. As a result, the 900-number industry's reputation became tarnished by fraud and abuse, and sales plummeted to $300 million annually. In 1992, pursuant to Congressional mandate, the FTC and the FCC promulgated rules to regulate the 900-number industry to ensure that consumers would receive price and other material information before incurring costs, and have

---

[1] My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any other Commissioner.

[2] 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty additional statutes, *e.g.*, the Clayton Act, 15 U.S.C. § 12, which prohibits various anticompetitive practices; the Truth in Lending Act, 15 U.S. C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; the Fair Credit Billing Act, 15 U.S. C. § 1666 *et seq.*, which provides for the correction of billing errors on credit accounts; and the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes rights with respect to consumer credit reports. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.* the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[3] Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

the right to dispute allegedly incorrect or unauthorized charges.[4] Annual sales began to climb again, reaching $450 million in 1995. The 900-number industry now seems poised to attract a higher volume of legitimate commerce because consumers can use 900-numbers with greater confidence.

Some of the same features that made pay-per-call technology a tempting field for fraud artists in the 1980s—low start-up costs and the potential for big profits—exist on the Internet today. Indeed, after buying a computer and modem, scam artists can establish and maintain a site on the World Wide Web for $30 a month or less and solicit consumers anywhere on the globe. There is nothing new about most types of Internet fraud the Commission has seen to date. What is new—and striking—is the size of the potential market and the relative ease, low cost, and speed with which a scam can be perpetrated.

If the Internet is to avoid a fate similar to that of 900-number technology, the Commission believes it is important to address Internet fraud now, before it discourages new consumers from going on-line and chokes off the impressive commercial growth now in progress and potential for innovation on the Internet. According to some industry analysts, total Internet business will climb from $2.6 billion in 1996 to $220 billion by 2001.[5] Much of this trade likely will involve business-to-business transactions. However, the on-line consumer market also is growing, and at an exponential rate. In early 1997, 51 million adults were already on-line in the U.S. and Canada.[6] Of those people, 73% reported that they had shopped for product information on the World Wide Web, the interactive graphics portion of the Internet.[7] By December 1997, the number of on-line users had risen to 58 million adults in the U.S. and Canada, and 10 million had actually purchased a product or service on-line.[8] Perhaps most telling, analysts estimate that Internet advertising—which totaled approximately $301 million in 1996—will reach $4.35 billion by the year 2000.[9]

If this trend and all the benefits that it implies are to continue, consumers must feel confident that the Internet is safe from fraud. Nothing is more likely to undermine their confidence than exploitation by scam artists using this new technology as yet another means to defraud consumers. Therefore, the Commission, like the Subcommittee, is concerned about fraud on the Internet and has taken strong action to combat it.

The Commission began to examine the potential for consumer protection problems on the Internet proactively, before on-line consumer transactions became common. In the fall of 1995, the Commission held public hearings to explore business and consumer issues arising from technological innovation and increasing globalization. Over 200 company executives, business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony. A two-volume report was published summarizing the hearings. Volume II, "Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace," reflects principles that many participants urged the Commission to consider when addressing the Internet and other technologies in the new Information Age:

> Consumer protection is most effective when businesses, government, and consumer groups all play a role. Meaningful consumer protection takes: (1) coordinated law enforcement against fraud and deception; (2) private initiatives and

---

[4] The FTC and the FCC promulgated their regulations pursuant to the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. §§ 5701 *et seq.* The FTC's regulations are at 16 C.F.R. Part 308; the FCC's regulations are at 47 C.F.R. § 64.1501 *et seq.*

[5] International Data Corporation, *Dramatic Growth of Web Commerce—From 2.6 Billion in 1996 to more than $220 Billion in 2001* (Aug. 26, 1997) (reported at http://www.idc.com/f/HNR/ic2001f.htm).

[6] CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old) (reported at http://www.commerce.net/work/pilot/nielsen—96/press—97.html) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS™): Second Quarter 1997 Study* (Sept. 4, 1997) (reported at http://www.intelliquest.com/about/release32.htm).

[7] *CommerceNet/Nielsen Demographic Study*, Spring '97.

[8] CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997) (reported at http://www.commerce.net/news/press/121197.html) [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. *See also*, Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (reported at http://www.yankelovich.com/pr/970327.HTM) (finding that 23% of users ordered and paid for a product over the Internet, *i.e.* "transacted" business online).

[9] Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (reported at http://wwwjup.com/digest/082297/advert.shtml) (figure includes directory listings and classified advertisements).

public/private partnerships; and (3) consumer education through the combined efforts of government, business, and consumer groups.[10]

Applying these principles, the Commission has taken the offensive against fraud on the Internet through a three pronged-strategy that emphasizes targeted law enforcement action, complemented by education of consumers and new Internet entrepreneurs, both of whom may be venturing into cyberspace for the first time. In all aspects of this strategy, but particularly in the Commission's consumer and business education efforts, the Commission has sought to form new partnerships with private industry and other government agencies, and the Commission has tried to turn new technologies to our advantage.

Law Enforcement

First and foremost, the FTC is a civil law enforcement agency with strong and effective enforcement tools to combat fraud and deception. The Commission can issue administrative complaints and conduct administrative adjudications that may result in the issuance of cease and desist orders against practices found to be unfair or deceptive.[11] Further, in cases of fraud and other serious misconduct, the Commission has statutory authority to file suit directly in federal district court to obtain preliminary and permanent injunctive relief, redress for injured consumers, or disgorgement of ill-gotten gains.[12] The Commission also may seek the assistance of the Department of Justice in filing criminal contempt proceedings against persons who violate court orders issued at the behest of the Commission, or in filing criminal actions in egregious fraud cases.

The Commission has brought over 25 law enforcement actions against defendants whose alleged illegal practices used or involved the Internet. Several of these cases involved alleged deceptive advertising and billing practices of commercial on-line service providers.[13] Most of the Commission's law enforcement actions, however, have involved old-fashioned scams dressed up in high-tech garb.[14] For example, the Commission has brought several cases to stop alleged pyramid schemes that recruit victims through the web.[15] In the Commission's largest Internet pyramid case to

---

[10] See Exhibit 1, Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace*, iii (May 1996).

[11] 15 U.S.C. §45.

[12] 15 U.S.C. §53(b). In addition, the Commission may request the Attorney General to file an action in the appropriate federal district court seeking civil penalties for violations of the Commission's administrative orders or trade regulation rules, and may file those actions on its own behalf if the Department of Justice declines to do so in the name of the United States. 15 U.S.C. §56.

[13] *America Online, Inc.*, FTC File No. 952–3331 (consent order subject to final approval, May 1, 1997); *CompuServ, Inc.*, FTC File No. 962–3096 (consent order subject to final approval, May 1, 1997); *Prodigy Services Corp.*, FTC File No. 952–3332 (consent order subject to final approval, May 1, 1997). These respondents allegedly made "free trial" offers to consumers without adequately disclosing that consumers would automatically be charged if they did not affirmatively cancel before the end of the trial period. (The Commission also alleged that AOL failed to inform consumers that 15 seconds of connect time was added to each online session, resulting in additional undisclosed charges, and that AOL misrepresented that it would debit customers' bank accounts only after receiving authorization to do so.)

[14] *E.g.*, ALLEGED CREDIT REPAIR SCAMS: *FTC* v. *Corzine*, No. CIV–S–94–1446 (E.D. Cal. filed Sept. 12, 1994); *FTC* v. *Consumer Credit Advocates, No. 96 Civ. 1990 (S.D.N.Y., filed Mar. 19, 1996); Martha Clark, d/b/a Simplex Services*, Docket No. C–3667 (consent order, June 10, 1996); *Bryan Coryat, d/b/a Enterprising Solution*, Docket No. C–3666 (consent order, June 10, 1996); *Lyle R. Larson, d/b/a Momentum*, Docket No. C–3672 (consent order, June 12, 1996); *Rick A. Rehem, d/b/a NBC Credit Resource Publishing*, Docket No. C–3671 (consent order, June 12, 1996). ALLEGED BUSINESS OPPORTUNITY SCAMS: *FTC* v. *Intellicom Services, Inc.*, No. 97–4572 TJH (Mcx)(C.D. Cal., filed June 23, 1997); *FTC* v. *Chappie (Infinity Multimedia)*, No. 96–6671–CIV-Gonzalez (S.D. Fla., filed June 24, 1996); *Timothy R. Bean, d/b/a D.C. Publishing Group*, Docket No. C–3665 (consent order, June 10, 1996); *Robert Surveys, d/b/a Excel Communications*, Docket No. C–3669 (consent order, June 12, 1996); *Sherman G. Smith, d/b/a Starr Communications*, Docket No. C–3668 (consent order, June 12, 1996). ALLEGED DECEPTIVE CASH GRANT MATCHING SERVICE: *Randolf D. Alberton, d/b/a Wolverine Capital*, Docket No. C–3670 (consent order, June 12, 1996). ALLEGED DECEPTIVE ADVERTISING OF HEALTH PRODUCT: *Global World Media Corp. and Sean Shayan*, Docket No. C–3772 (consent order, Oct. 9, 1997). ALLEGED MISREPRESENTATIONS ABOUT PRODUCT CHARACTERISTICS: *Zygon International, Inc.* Docket No. C–3686 (consent order, Sept. 24, 1996). ALLEGED NON-DELIVERY OF ORDERED MERCHANDISE: *FTC* v. *Brandzel*, 96 C. 1440 (N.D. Ill., filed Mar. 13, 1996).

[15] *E.g.*, *FTC* v. *The Mentor Network, Inc.*, Civ. No. SACV96–1104 LHM (EEx) (C.D. Cal., filed Nov. 5, 1996); *FTC* v. *Global Assistance Networkfor Charities*, Civ. No. 96–02494 PHX RCB (D. Ariz., filed Nov, 5, 1996); *FTC* v. *JewelWay International, Inc.*, CV97–383 TUC JMR (D. Ariz., filed June 24, 1997); *FTC* v. *Rocky Mountain International Silver and Gold, Inc.*, Action No. 97–WY–1296 (D. Colo., filed June 23, 1997).

date, *FTC* v. *Fortuna Alliance*,[16] the defendants allegedly promised consumers that, for a payment of $250, they would receive profits of over $5,000 per month. The program spawned numerous web sites on the Internet and appealed to victims all around the globe seeking to get rich quickly for little effort. Yet sheer mathematics dictated that 95 percent of the consumers who joined the program could never make more than they paid in. The Commission obtained a temporary restraining order halting the unlawful practices and freezing the assets of the individuals who developed and operated the Fortuna program. The court order also required the defendants to repatriate the assets they had deposited overseas. In February 1997, the defendants stipulated to a permanent injunction that prohibited their alleged pyramid program and provided for redress to consumers who requested refunds. The defendants subsequently balked at paying many consumers, and the Commission filed a contempt motion. The court did not impose sanctions but issued a compliance order against the defendants on January 6, 1998. The compliance order clears the way for over 8,600 Fortuna members to begin receiving refunds.

Another alleged Internet pyramid scheme targeted in a recent Commission law enforcement action was Credit Development International.[17] The scheme was propelled by allegedly false promises that those who joined CDI would receive an unsecured Visa or MasterCard credit card with a $5,000 limit and a low interest rate, as well as the opportunity to receive monthly income of $18,000 or more. The Commission filed its complaint on October 29, 1997, and on October 31, the court granted a temporary restraining order, appointed a receiver to oversee the corporate defendants, and froze both the corporate and individual defendants' assets. After a hearing, on November 20, 1997, the court issued a preliminary injunction against the defendants. The Commission's staff estimates that over 30,000 consumers collectively may have lost 3 to 4 million dollars in this alleged scam. This matter is still in litigation.

The Commission's investigators discovered the Credit Development International scam as part of an ongoing effort to monitor "spam"—also known less colloquially as unsolicited commercial e-mail ("UCE")—on the Internet. One theme sounded in the Commission's recent privacy hearings was that an ever-increasing volume of UCE strains the capacity of on-line service providers and threatens the development of the Internet as a conduit for commerce. For example, at the Commission's privacy hearings held in June 1997, America Online ("AOL") reported that it handled 15 million electronic messages per day. By September 1997, that number had quadrupled to 60 million messages per day. Significantly, AOL has estimated that UCE comprises as much as one-third of all e-mail traffic.

Beyond the sheer volume and potential annoyance of UCE, many UCE messages may be misleading or deceptive.[18] Alleged scams like Fortuna and Credit Development International generate huge quantities of UCE, because e-mail is unparalleled as a means of cultivating a "downline"—additional recruits to a pyramid—for virtually no cost and little effort. The same attributes make UCE attractive to other types of scams as a means to solicit millions of consumers for little cost.

Although most Internet fraud is fairly traditional, the Commission has taken action against one scheme that uniquely and ingeniously exploited what can be done on the Internet and *only* on the Internet. The case *FTC* v. *Audiotex Connection, Inc.*, CV–97 0726 (DRH) (E.D.N.Y.), presented a scheme that allegedly "hijacked" consumers' computer modems by surreptitiously disconnecting them from their local Internet Service Provider (such as AOL) and reconnecting them to the Internet through a high-priced international modem connection, purportedly going to Moldova but actually terminating in Canada. On various Internet sites, the defendants offered access to free computer images through a special "viewer" program. If a consumer downloaded and activated the viewer software, the alleged hijacking automatically ensued, and an international long-distance call (and the charges for it) continued until the consumer turned off the computer—even if he or she left de-

[16] Civ. No. C96–799M (W.D. Wash., filed May 23, 1996).

[17] *FTC* v. *Nia Cano d/b/a Credit Development Int'l & Drivers Seat Network*, No. 97–7947 IH (AJWx) (C.D. Cal. filed Oct. 29, 1997).

[18] In addition, UCE often contains fake or altered routing information in the address portion of a message, *i.e.*, the "From," "Received from," or "Reply to" lines. Thus, consumers may not know who sent the e-mail or to whom they should reply. Fake "Reply to" lines also may send undeliverable or reply messages back to the wrong address, thereby tying up a legitimate business's computer. This may confuse consumers, but in addition, UCE may directly deceive them through misleading advertisements or solicitations that appear in the body of the e-mail itself. The Commission has received, directly or by referral from consumers, over 50,000 UCE messages. Our staff actively reviews these messages and investigates purveyors of UCE that may violate the FTC Act's prohibition against unfair or deceptive practices.

fendants' sites and moved elsewhere on the Internet, or left the Internet entirely to use a different computer program.

Commission staff were first alerted to the *Audiotex* scheme by security experts at AT&T. The United States Secret Service assisted staff in ascertaining how this "Trojan horse" viewer software worked, and AT&T lent further assistance in tracing the software back to specific web sites. With this help, the Commission's staff completed its investigation, filed a complaint, and obtained an *ex parte* temporary restraining order and asset freeze against the defendants within just 31 days of learning about the alleged scam. The lawsuit was recently resolved by entry of a stipulated permanent injunction against the main defendants named in the Commission's complaint and the issuance of a virtually identical administrative order against additional parties found to have played a role in the alleged scam. Under the two orders, the defendants and administrative respondents are barred from engaging in the alleged unlawful practices, and over 38,000 consumers should receive full redress worth an estimated $2.74 million.[19]

Consumer Education

The Commission has gone on-line to reach Internet users. Since April 1995, the Commission has used its web site at "www.ftc.gov" to make instantly available to consumers a rich and continuously updated body of advice and information. The Commission receives approximately 60,000 to 75,000 "hits" per day on this home page.[20] In September 1997 alone, FTC.GOV received almost 2 million hits from 114,000 visitors.

In constructing its web site, the Commission has put a premium on making it not only comprehensive, but also user-friendly. FTC.GOV contains a search engine that allows consumers to pull up information by typing in a few key words. The site also contains a special section called ConsumerLine that provides news releases, consumer alerts, and on-line versions of all of the Commission's consumer and business education publications.[21]

Building on the success of the FTC's home page, the Commission's staff conceived a plan to create a new site at "www.consumer.gov" and has developed the site in partnership with sister agencies—the Securities and Exchange Commission ("SEC"), the U.S. Consumer Product Safety Commission ("CPSC") the Food and Drug Administration ("FDA"), and the National Highway Traffic Safety Administration ("NHTSA"). CONSUMER.GOV provides the public with "one-stop shopping" for federal information on a broad spectrum of consumer issues, ranging from auto recalls to drug safety to investor alerts.[22]

Extending a hand to consumers at their most vulnerable point—when they are surfing in areas of the Internet likely to be rife with fraud and deception—the staff of the Commission has posted several "teaser" web sites. The "Ultimate Prosperity Page" is one example advertising a fake deceptive business opportunity. The "Ultimate Prosperity Page" uses "buzz words" and promises of easy money common to many such scams. When the consumer clicks from the "Ultimate Prosperity Page" to the next page in the series, he or she finds glowing testimonials from fictitious persons who purportedly have achieved fabulous success through the business opportunity—again mirroring the typical get-rich-quick business opportunity scam. Clicking through to the third and final page in the series, however, brings the consumer to a sobering warning: "If you responded to an ad like [this], you could get scammed." The warning page gives advice on how to avoid fraudulent business opportunities and provides a hyper-text link back to FTC.GOV, where consumers can learn more about investing in franchises or business opportunities.[23]

There are now other teaser sites, posted by the Commission's staff, that mimic pyramid schemes, scholarship scams, deceptive travel programs, false weight-loss claims, and fraudulent vending opportunities—all perennial frauds that have been practiced on consumers for years through direct mail, telemarketing, and other means, and are now enjoying new life on the Internet.[24] The Commission's staff has registered each "teaser" site with major search engines and indexing services on the

[19] The Commission would like to acknowledge the assistance of AT&T and MCI in administering the redress program. AT&T and MCI will distribute refunds to most consumers in the form of telephone credits on their long-distance telephone bills.

[20] A "hit" occurs when someone accesses a web site.

[21] After the home page for FTC.GOV, the search engine is the most popular area visited on the web site, followed by the ConsumerLine section. *See* Exhibit 2, excerpts from "www.ftc.gov".

[22] Exhibit 3, homepage of "www.consumer.gov".

[23] To alleviate any privacy concerns that consumers may hsve, the warning page makes it clear that the FTC has not gathered any personal information about individuals visiting this teaser site.

[24] Exhibit 4, examples of FTC teaser sites.

Internet. Thus, consumers may encounter the site when they are perhaps most receptive, just when they may be about to become ensnared in a fraud by responding to a plausible but untrue come-on. Private on-line service companies have worked with the Commission's staff to highlight various teaser pages and have billed some as the "new" or "cool" site of the week.[25]

In another effort to use new technology to reach the public, the staff of the Commission partnered with the North American Securities Administrators Association and held a real time on-line forum on the Internet in April 1997. Over 100 consumers participated, posing questions to, and receiving instantaneous responses from, state and federal experts about how to invest wisely in new business ventures or franchises. The Commission posted the transcript of this "chat" session on its web site so that other consumers could access it and benefit from the exchange.

The Commission has actively sought Internet companies and trade groups to join with us as partners in disseminating consumer protection information to consumers on-line. As a result, the Interactive Services Association, a leading on-line trade association, and companies such as AT&T, NetCom, and America Online have helped circulate public service announcements over the Internet, cautioning consumers to avoid particular scams and "hot linking" consumers to the Commission's web site where they can find "Cybershopping" guides, "Safe Surfing" tips, and other helpful information.

Business Education

At the forefront of its business education efforts, the Commission has conducted a number of "Surf Days" aimed at providing information to new entrepreneurs who may unwittingly violate the law. The first Surf Day was conducted in December 1996 and focused on pyramid schemes that had begun to proliferate on the Internet. Commission attorneys and investigators enlisted the assistance of the SEC, the U.S. Postal Inspection Service, the Federal Communications Commission, and 70 state and local law enforcement officials from 24 states. This nation wide *ad hoc* task force surfed the Internet one morning, and in three hours, found over 500 web sites or newsgroup messages promoting apparent pyramid schemes. The Commission's staff e-mailed a warning message to the individuals or companies that had posted these solicitations, explaining that pyramid schemes violate federal and state law and providing a link back to FTC.GOV for more information. In conjunction with the New York Attorney General's Office and the Interactive Service Association, the Commission announced the results of Internet Pyramid Surf Day at a televised press conference held during the Internet World '96 convention in New York City. A month later, the Commission's investigative staff checked on the status of web sites or newsgroups identified as likely pyramids during Surf Day and found that a substantial number had disappeared or been improved.[26] The Commission has employed this technique several times since, conducting additional Surf Days focused on Internet web sites or newsgroup messages that promoted potentially problematic business opportunities, credit repair schemes, and "miracle cure" health products.

The Commission has now taken its Surf Day concept to the private sector, the global law enforcement community, and sister agencies as well. In August 1997, the Coupon Information Center, a private trade association, and its members from the national merchandising community joined Commission staff in surfing for fraudulent opportunities that promoted coupon certificate booklets. Then on October 16, 1997, the Commission helped coordinate the first "International Internet Surf Day." Agencies from 24 countries joined this effort and targeted "get-rich-quick" schemes on the Internet.[27] Australia's Competition and Consumer Commission oversaw the world-wide effort while the FTC led the U.S. team consisting of the SEC, the Commodities Futures Trading Commission ("CFTC") and 23 state agencies.

In November 1997, the Commission used the Surf Day concept to help the Department of Housing and Urban Development ("HUD") target unscrupulous "HUD Tracers." These "tracers" track down consumers to whom HUD may owe a refund for FHA mortgage insurance. Consumers can claim their refund for free by contacting

[25] Exhibit 5, example of FTC teaser site highlighted as "new" site of the week by Yahoo!, a large Internet search engine and indexing service.

[26] Apart from newsgroup messages that had terminated automatically, 66 (18%) of the notified web sites had been improved or taken down within a month. In the wake of a subsequent Surf Day that targeted a separate type of fraud, 24% of the notified web sites improved or removed their solicitations.

[27] International participants included Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Hungary, Ireland, Jamaica, Japan, Korea, Mexico, New Zealand, Norway, the Philippines, Poland, Portugal, South Africa, Spain, Sweden, Switzerland, and the United Kingdom.

HUD directly; however, unscrupulous "tracers" may falsely claim that refunds cannot be secured without their assistance (and they may charge up to 30 percent in commissions), may falsely claim an affiliation with the government, and may falsely represent to other entrepreneurs how much money they can make as "HUD tracers." The HUD Tracer Surf Day not only helped to generate publicity to inform consumers about HUD's refund program, but it also helped eliminate many potentially deceptive solicitations from the Internet. A month after sending out warning messages, the Commission's staff checked on suspect tracer sites and found that 70 percent had shut down entirely or removed questionable claims about earnings potential or their affiliation to HUD.

Earlier this month, the Commission announced yet another innovative use of the Surf Day concept, this time targeting deceptive UCE messages. Commission staff conducted a "fall harvest" by surfing the Commission's large database of UCE solicitations, topic by topic, and identifying over 1000 individuals or companies potentially responsible for misleading e-mail solicitations, for example, for pyramid or other get-rich-quick schemes. Ironically, most of these UCE messages did not allow any reply by e-mail, due to inaccurate or deceptive "sender" information, so in January through the U.S. Postal system the Commission sent out letters warning the sources of the UCE that their messages may be in violation of the law.

Our messages to businesses on the Internet are straightforward—*e.g.*, don't lie or make misleading statements; don't make product or earnings claims that you can't support, don't mislead consumers with unrealistic testimonials. The difficulty lies in finding a way to get these basic messages to new entrepreneurs who may have no prior business or advertising experience. Surf Days help us overcome this hurdle, but in addition, we have put together a "road show" that our ten regional offices can use in their local communities to help explain how basic legal principles apply on the Internet. The Commission also is preparing a business guide for Internet entrepreneurs and a continuing legal education ("CLE") course for lawyers who counsel new Internet businesses. Finally, the Commission is going directly to the computer industry for help. In July, Commission representatives met with Silicon Valley executives at Stanford University's Technology and Business Strategy Summit '97, and asked them to lend us their contacts and marketing expertise in order to reach new Internet entrepreneurs.

Looking Ahead

Currently, the Commission receives approximately 100 to 200 Internet-related complaints per month. Many of these complaints are forwarded to us by the National Fraud Information Center, with which the Commission works closely. The Commission has seen an increase in complaints over the last year, but fortunately on-line problems seem to be growing at a slower pace than the Internet marketplace itself. At the moment, complaints about Internet fraud remain a small fraction of the number of complaints the Commission receives about more traditional problems concerning credit cards or telemarketing. However, the Commission expects that as the Internet marketplace grows, reports about consumer fraud also will continue to grow.

The potential for fraud is likely to be fueled by easy on-line access that exists for legitimate and fraudulent businesses alike. Also, it is likely that many first-time entrepreneurs, because of their lack of marketing experience or knowledge of their obligations under basic consumer protection principles, will unwittingly engage in Internet practices that violate the law. Finally, keeping up with the introduction and application of new technologies will prove daunting. The growing problem of "spam" already threatens to outstrip our resources. The Commission currently receives approximately 500 pieces of UCE per day, forwarded by disgruntled consumers and others—far more than we can read or analyze on an individual basis and a volume that strains the capacity of the agency's computers.

Mr. ROGAN [presiding]. Ambassador Aaron, welcome to the subcommittee.

STATEMENT OF AMBASSADOR DAVID AARON, UNDER SECRETARY OF COMMERCE FOR INTERNATIONAL TRADE, U.S. DEPARTMENT OF COMMERCE

Mr. AARON. Thank you very much, Mr. Chairman.

The Clinton Administration appreciates the opportunity to testify on Administration policies related to information privacy. I am accompanied today by Becky Burr, the Acting Associate Adminis-

trator for the National Telecommunications and Information Administration of the Department of Commerce, and Barbara Wellbury, Special Counsel for Electronic Commerce in our General Counsel's Office, both of whom have major responsibilities in this field.

Americans treasure privacy. It's fundamental to our concept of personal well-being and our concept of liberty. The Internet's great promise, that it facilitates the collection, re-use and instantaneous transmission of information, can also, if not managed carefully, diminish personal privacy. It's essential, therefore, to assure personal privacy in the networked environment.

At the same time, fundamental and cherished principles like the First Amendment protect the free flow of information. Commerce on the Internet will thrive only if the privacy rights of individuals are guaranteed and also balanced with the benefits associated with the free flow of information.

The Clinton Administration has been aggressive about privacy protection in general and the Internet in particular. Apart from the Internet, the Administration has called for legislation to protect the privacy of medical records and genetic information. Moreover, the Administration supported the 1996 amendments to the Fair Credit Reporting Act that extended the coverage of the Act to hundreds of information providers to strengthen privacy protection of financial information generally. And we supported adoption of new limits on the use of telephone subscriber information by telephone common carriers in the Telecommunications Act of 1996. Moreover, we also supported the Drivers' Privacy Protection Act of 1994 which governs how states make motor vehicle and licensed driver information available. And of course we have supported the efforts of the FTC just described by Mr. Medine.

I want to stress in this connection that existing applicable statutory protections, such as the Fair Credit Reporting Act and the others I just mentioned, apply to personally identifiable information on the Internet. The obligations to protect privacy do not change just because the medium is electronic.

The Clinton Administration is concerned, however, that the nature of the Internet reduces the effectiveness of legislative and regulatory solutions. Congress could certain pass a law mandating privacy protections on the Internet, but enforcement of such a law, even if possible, might require enormous resources. We don't want to give Internet users a false sense of security based on an unenforceable law.

Instead, as set forth in A Framework for Global Electronic Commerce, the Clinton Administration supports private sector efforts to implement meaningful, consumer friendly, self-regulatory regimes based on fair information practice principles. Fair information practice principles include consumer awareness, choice, appropriate levels of security, and consumer access to their personally identifiable data.

Consumer awareness of information practices is a first step in advancing on-line information privacy. At a minimum businesses must develop and post prominently, clearly- written policies that inform consumers about the identity of the collector of their per-

sonal information, intended users of this information, and the means by which consumers may limit its disclosure.

Consumers must also have readily available simple and affordable opportunity for exercising choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties.

Security of information is critical if electronic commerce is to flourish. Companies with records of identifiable personal information must take reasonable measures to assure their accuracy and must take reasonable precautions to protect them from loss, misuse, alteration or destruction.

Consumers must have reasonable access to information about them that is held by businesses and should have a right to correct or amend that information.

Let me be clear: to be meaningful self-regulation must be more than an articulation of broad policies and guidelines. Self-regulatory privacy regimes must provide consumers with simple, readily available and affordable enforcement mechanisms to assure compliance when rules are not followed. Enforcement mechanisms may vary depending on the type and nature of the company and the kind of information the collection uses. But in the end we think that enforcement mechanisms will provide at least three elements: consumer recourse, verification and consequences, and let me speak to each of them.

Consumer recourse. Companies that collect and use personally identifiable information should offer consumers readily available and affordable mechanisms by which their complaints can be resolved.

Second, verification. Verification provides assurances that a company's privacy practices have in fact been implemented as represented.

Third, consequences. For self-regulation to be effective, failure to comply with fair information practices must have consequences, such as posting the name of a non-complier on a publicly-available "bad actors" list or forfeiting membership in a trade association. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may also be liable for fraud and subject to action by the Federal Trade Commission.

On July 1st the Commerce Department and OMB will report to the President on private sector implementation of self-regulation for privacy. We are looking for industry leadership to ensure that privacy codes of conduct are easy for consumers to recognize, comport with fair information practices, provide for verification of compliance, provide prompt and efficient dispute resolution and recourse for consumers harmed by misuse of personal information, and provide appropriate consequences for those who violate privacy policies.

I'll stop there, Mr. Chairman, and be prepared to answer your questions.

[The prepared statement of Ambassador Aaron follows:]

PREPARED STATEMENT OF AMBASSADOR DAVID AARON, UNDER SECRETARY OF COMMERCE FOR INTERNATIONAL TRADE, U.S. DEPARTMENT OF COMMERCE

SUMMARY

Americans treasure privacy, linking it to our concept of personal freedom and well-being. The Internet's great promise can also, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

The Clinton Administration has been aggressive about privacy protection in general and on the Internet in particular. For example, it called for legislation to protect the privacy of medical records and genetic information. And, while existing statutory protections and regulatory obligations apply to personally identifiable information on the Internet, the Administration has been worked to find alternative approaches because the Internet by its nature reduces the effectiveness of legislative solutions.

The Clinton Administration supports private sector efforts to implement effective consumer-friendly, self-regulatory policies. These should be based on fair information practices and provide consumers with the means to know the rules, that companies comply with them, and that consumers have an appropriate means of redress when injuries result from noncompliance.

On July 1 the Commerce Department and OMB will report to the President on efforts by the private sector to implement privacy protections. We look to industry leadership to provide effective and enforceable privacy codes of conduct that comport with fair information.

The Administration considers privacy protection critically important. We believe that private efforts of industry working in cooperation with consumer groups can be more effective and are preferable to government regulations, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.

STATEMENT

Mr. Chairman and members of the House Judiciary Committee, I am David Aaron, Under Secretary, International Trade Administration of the U.S. Department of Commerce. The Clinton Administration appreciates the opportunity to testify on our policies related to information privacy. As outlined in his Directive on Electronic Commerce, President Clinton instructed the Department of Commerce and the Office of Management and Budget to lead the Administration's privacy efforts and to encourage private industry and privacy advocacy groups to adopt effective self regulatory approaches to protect privacy on the Internet. As Under Secretary of ITA, I am deeply involved in many aspects of the our electronic commerce initiatives, including privacy policy.

Americans treasure privacy, linking it to our concept of personal freedom and well-being. The Internet's great promise—that it facilitates the collection, re-use, and instantaneous transmission of information—can also, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

At the same time, fundamental and cherished principles like the First Amendment protect the free flow of information. Commerce on the Internet will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information.

The Clinton Administration has been aggressive about privacy protection in general and the Internet in particular. Apart from the Internet, for example, the Administration called for legislation to protect the privacy of medical records on genetic information. In addition, the Administration supported 1996 amendments to the Fair Credit Reporting Act that extend the coverage of the Act to hundreds of information providers and strengthens financial privacy. In the Telecommunications Act of 1996, the Administration supported new limits on the use of telephone subscriber information by telephone common carriers. Additionally, the Administration supported passage of the Drivers' Privacy Protection Act of 1994, which governs how states make motor vehicle and licensed driver information available.

Specific sectoral privacy statutes, such as those mentioned above apply to information on the Internet. But because networked communication technology facilitates data collection and sharing, privacy concerns are heightened with regard to the Internet. *I want to stress that existing applicable statutory protections and regulatory obligations apply to personally identifiable information on the Internet.*

The Clinton Administration is concerned, however, that the nature of the Internet makes legislative and regulatory privacy protections less effective on-line. On the World Wide Web, new sites appear and others disappear at an astonishing rate.

Congress could certainly pass a law mandating privacy protections on-line, for example, but enforcement of such a law, even if possible, might require enormous resources. We don't want to give Internet users a false sense of security based on an unenforceable law.

Therefore, the Clinton Administration has also been active with respect to the specific issues of protecting privacy on the Internet. In 1993, the Administration set up the Information Infrastructure Taskforce (IITF), a cabinet level group charged with articulating and implementing the Administration's program, to promote the development of the Information Superhighway; the group was chaired by the late Secretary of Commerce, Ron Brown. The Clinton Administration quickly realized that successful development of the information infrastructure would require enhanced privacy protections. Quite simply, while the infrastructure might get built, consumers will not use it until their personal data is adequately protected. Accordingly, in 1995, the IITF examined privacy in the electronic environment and issued Privacy Principles updated for the information age.

The Privacy Principles were developed with substantial input from industry and consumer groups. They provide a general framework from which more specific laws and quidelines could be written for particular sectors of the economy or to remedy particular abuses. The Principles explicitly call upon the private sector to develop detailed guidance responsive to particular needs of the individual sectors.

Similarly, when the Administration issued its policy statement on electronic commerce, *A Framework for Global Electronic Commerce*, it supported private sector efforts to implement meaningful, consumer-friendly, self-regulatory regimes based on the fair information practice principles. (These principles were contained in a report presented in 1973 to the then Department of Health, Education and Welfare, now the Department of Health and Human Services; adopted by the international community in the early 1980s in the form of the OECD's Guidelines for the Protection of Personal Data and Transborder Data Flows; and formed the basis for the Privacy Principles.) They include consumer awareness, choice, appropriate levels of security, and consumer access to their personally identifiable data.

Consumer *awareness* of information practices is essential to promoting on-line information privacy. Information about their rights and responsibilities in personal data enables consumers to make judgments about the levels of privacy available to them and to make meaningful choices about the use of their data. At a minimum, consumers must know the identity of the collector of their personal information, the intended uses of the information, and the means by which consumers may limit its disclosure. Accordingly, businesses must develop policies that articulate the manner in which they collect, use, disclose, and protect data, and the choices they offer consumers to exercise rights in their personal information. Notice of companies' information practices is a first principle in advancing privacy. Notification must be written in language that is clear and easily understood, and must be displayed prominently and in a manner that allows consumers to access it prior to relinquishing information to the company.

Consumers must be given the opportunity to exercise *choice* with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers must be provided with a simple, readily available, and affordable mechanism—whether through technological means or otherwise—to exercise this option. For certain kinds of information, e.g., information related to children, affirmative choice by consumers may be appropriate—personal information may not be used by companies unless it is specifically released by the individual or his or her parent or guardian.

Security of information is critical if electronic commerce is to flourish. Companies creating, maintaining, using or disseminating records of identifiable personal information must take reasonable measures to assure their reliability for their intended uses and must take reasonable precautions to protect them from loss, misuse, alteration or destruction. Companies should also strive to assure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to its own.

Consumers must have reasonable *access* to information about them that is held by businesses, and should have a right to request corrections and amendments of that information. Mechanisms must be in place to make it possible to exercise that right, although the extent of access may vary from industry to industry. Decisions about the level of appropriate access necessarily must take into account a number of factors, such as the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, the ways in which the information is to be used, and the cost of access.

Let me be clear: to be meaningful, self regulation must be more than an articulation of broad policies or guidelines. Effective self regulation must involve sub-

stantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have an appropriate means of redress for injuries resulting from noncompliance.

A self-regulatory regime to protect privacy must have some enforcement mechanism to assure compliance with the rules and appropriate redress to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their rights in data, and must, therefore, be readily available and affordable. They may take several forms, and businesses may need to use more than one of these tools depending upon the nature of the enterprise and the kind of information the company collects and uses. But in the end, we think that enforcement mechanisms will provide at least three elements: consumer recourse, verification, and consequences.

1. *Consumer recourse.* Companies that collect and use personally identifiable information should offer consumers a mechanism by which their complaints can be resolved. Such mechanisms must be simple, readily available, and affordable.

2. *Verification.* Verification provides attestation that the assertions businesses make about their privacy practices are true, and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of information with which a company deals—companies using highly sensitive data may be held to a higher standard of verification.

3. *Consequences.* For self regulation to be effective, failure to comply with fair information practices must have consequences. Among these may be cancellation of the right to use a certifying seal or logo, posting the non-complier on a publicly available "bad-actors" list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining its noncompliance. Ultimately, sanctions should be stiff enough to be meaningful, and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so they may be liable for fraud and subject to action by the Federal Trade Commission.

On July 1, the Commerce Department and OMB will report to the President on private sector implementation of effective self regulation for privacy, including codes of conduct, industry developed rules, technological solutions to protect privacy on the Internet, and means for ensuring the privacy of children online. *We are looking for a commitment from industry to establish enforcement mechanisms to ensure that sector-specific self regulatory codes (1) are easy for consumers to recognize, (2) comport with fair information practices, (3) verify compliance through audits or other procedures, (4) provide prompt and efficient dispute resolution and recourse for consumers harmed by misuse of personal information, and (5) provide appropriate consequences (trade association disciplinary measure, revocation of seals, etc.) for those who violate privacy policies.*

In anticipation of this report, the Department of Commerce will hold a privacy conference in May. This two-day DOC conference will bring together the private sector and consumer groups to work toward establishing enforcement mechanisms for privacy self regulation. The conference will serve several purposes. First, it will raise consumer awareness of privacy issues; second, it will allow companies to begin to present the status of their efforts toward self regulation; third, it will allow a full and fair discussion of the role that self regulation can play in online privacy protection; fourth, it will allow presentation and public discussion of enforcement mechanisms self regulation; and fifth, it will set the stage for further evaluation of privacy protection technology.

The Department of Commerce will follow up the May conference by continuing the dialogue with industry and consumer groups in a variety of informal and perhaps more formal ways.

The Administration considers privacy protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.

That concludes my comments on the issue of privacy. I will be happy to answer any questions.

Mr. COBLE. I thank you both for your testimony. Pardon my abrupt departure. I had to go to the Crime Subcommittee for a markup. It was not that I was not interested in what you all were saying.

Ambassador, what sort of response are you getting from businesses to the Administration's policy statement regarding the im-

plementation of fair information practice principles, or in a more simplified way is the business/commercial community taking adequate steps to implement these principles?

Mr. AARON. We are encouraged, Mr. Chairman. The Secretary of Commerce has met with me personally on two occasions. We will have further meetings to encourage a positive industry response. We believe that by the time we make our report to the President on July 1 that we will have something positive and concrete to present to him.

In addition, the Commerce Department is holding a conference in May which will offer an opportunity for business, interested nongovernmental organizations, privacy organizations and the rest to come together and begin the process of evaluating the steps that businesses are taking. I think that as we prepare the report to the President we will have an opportunity to see in more concrete terms what industry is proposing to do.

Mr. COBLE. Ambassador, currently what type of consumer recourse is available to members of the public when they have had their privacy rights violated?

Mr. AARON. If I may, I would like to turn to Ms. Burr to respond to that.

Mr. COBLE. Sure, that's fine.

Ms. BURR. Thank you very much. Aside from the protections that the Federal Trade Commission offers with respect to deceptive practices and unfair practices in commerce, there is not yet widespread, systematic consumer recourse. That is something that we are very much expecting to be developed in the coming months. The Secretary in his visits with members of the business community has indicated some need to hasten the process, and we believe that there are several models. For example, the Better Business Bureau online is providing some dispute resolution services, and there are a couple of other models. But I would have to say at this point there is not outside of the Federal Trade Commission widely available, simple-to-use dispute resolution procedures.

Mr. COBLE. Thank you.

Mr. Medine, in your written testimony you indicate that the Internet as a commercial entity likely will not flourish until the public is assured that their personal information is protected, and I'm inclined to agree with that conclusion.

On our second panel today we will hear from witnesses who will advocate a hands-off approach by the Congress. Now how do you respond to that admonition?

Mr. MEDINE. Well, we do believe that electronic commerce provides some tremendous opportunities, and we really are at a crossroads right now as to whether this marketplace will develop or not. What we've heard from consumers through surveys and through our workshops is that they are very concerned about their privacy online, and many consumers are reluctant to shop online and don't even go online because of privacy concerns.

So the question is how do you protect that privacy online? The approach that we've taken in response to industry's request, is to encourage self-regulation, to facilitate and provide forums in which all interested parties are able to sit at the same table and discuss these important issues. We think that industry self-regulation can

provide tremendous flexibility, can adapt to changing technology, and limit the use of government resources in trying to accomplish these ends. But self-regulation has to be effective to provide these protections or this marketplace will not flourish.

That's the reason why this month we are surveying 1,200 web sites to get a sense, after 3 years of working with industry to try to facilitate an awareness of this issue, whether it has taken hold and whether companies are providing consumers adequate disclosures of privacy policies, and when we report to the Congress in June on this we will have a sense of whether that has worked or not.

Mr. COBLE. Mr. Medine, will you elaborate on the FTC public workshops' efforts to educate parents on the dangers of having their children's information on the Internet. Bring us up to speed on that.

Mr. MEDINE. I would be happy to. The Commission has historically devoted special attention to protecting children in commerce. The Internet provides an unprecedented ability not only to give information to children, but to gather information from children without the intervention of their parents, and that raises special concerns for the Federal Trade Commission because of the possible misuse of that information by pedophiles and others.

So we have devoted a lot of attention in our public workshops to highlighting the extent to which technology can protect children. But, we have also issued a staff opinion letter stating that the Federal Trade Commission Act does apply to the collection and distribution of information from children on the Internet in two particular ways.

First, if information is gathered from young children and there is not adequate disclosure of how that information is going to be used and why that information is being collected, we believe that to be a deceptive trade practice under current law.

We also believe that if information is gathered from children for distribution to third parties that poses a special risk to the child and that parental consent is required in that instance before the information is distributed to third parties, and failure to obtain parental consent is an unfair trade practice under the Federal Trade Commission Act.

We also have encouraged industry efforts to provide further protections and notice to children, but we believe there is a base legal authority that currently applies to the very sensitive issue of gathering information from children on the Internet.

Mr. COBLE. Thank you, Mr. Medine.

The gentleman from Massachusetts, Mr. Frank.

Mr. FRANK. Well let me begin with that, and, first, I want to thank the witnesses for helping us in this. You said there is a basic legal authority that covers this, and would you elaborate on that.

Mr. MEDINE. It has not yet been tested in court, but the staff has issued an opinion that the Federal Trade Commission Act's deception and unfairness authorities do apply in particular to the gathering of information from young children.

Mr. FRANK. And the unfairness aspect of it?

Mr. MEDINE. Unfairness looks primarily toward injury that can't be easily avoided, and we believe that gathering information from

children on the Internet when it's being distributed to third parties presents a special risk to children and that it is an unfair trade practice unless parental consent is obtained.

Mr. FRANK. Is there an effort to find an appropriate test case going on?

Mr. MEDINE. We are currently investigating online firms for their practices regarding collection of information from children and do expect enforcement actions in this area in the future.

Mr. FRANK. The reason I ask is that I would think as we begin to look for areas where we could act that would be one where we have run into this situation. This would be one where we will get a lot of fake reasons, and fake reasons play a very important role in the legislative process. Fake reasons are what you put forward when you don't think your real reason will stand the light of day, and it often happens in legislative debates. People will express reasons why something shouldn't be passed, it is unnecessary, it's confusing, it doesn't go far enough or it goes too far. I expect that if we were to try to legislate protection for children we would hear from a lot of businesses that now make money from this information from children and we would hear a lot of their fake reasons, and their real reason would be they want to continue to make money off children.

I think that's an area where we'll be legislating. So I'll be interested to see what your result is. But I would also say people who might be inclined vigorously to contest your enforcement efforts on the grounds that you don't have sufficient statutory authority should be aware that they will be helping us make the case for a more explicit statutory authority. So people should understand that. I'm glad that you're planning to go ahead, and if your efforts should be frustrated by some legal interpretation, then we are talking about our statutory right.

In fact, let me ask all of the witnesses. One of the things we hear from the private business community is, oh, don't worry, we can do self-regulation. I take from you, Mr. Medine, because you are talking about proceeding legally, you obviously do not accept that argument; is that correct?

Mr. MEDINE. Well, I think there are two issues there. I mean there are always going to be firms that don't comply with the law, and that's when enforcement actions are appropriate. But the question is whether the bulk of industry is voluntarily providing protections to consumers.

Mr. FRANK. You said complying with the law, but self-regulation I assume means there is no law. I mean the argument for self-regulation is we're here in a new medium, and we have people saying we don't need any laws, we are the good citizens of cyberspace. This is a Lockean state of nature and not a Hobbesian one. We all get along and everybody is going to be fine and wonderful and we'll respect each other's rights. Maybe it's even Rousseauean. Locke would require too much government. I take it you are implicitly rejecting that saying we do need some law.

Now I think there are two obvious questions. One is do you need any law at all. There is nobody here but us well-motivated anarchists who say you don't need any law at all. Then there is a second-level question which is given the basic legal structure how in-

tensive an enforcement effort do you need, and that's when I think the question about voluntary compliance or not would come in.

But I would hope that we would have some agreement that this notion that we don't need any law just doesn't work, and that if you have the law we would then hope that most people would comply voluntarily. That's the way we tend to prefer law enforcement.

Mr. MEDINE. Well I think the question is where does the law currently begin and end? I think, following up on Becky Burr's comments, FTC's authority primarily in the adult area relates to deception, which is a firm states how they are going to be using information; we can enforce that by bringing an action. What we can't mandate is a firm stating their privacy policies. They have to do that voluntarily.

Mr. FRANK. Right.

Mr. MEDINE. So that's where industry self-regulation comes in.

Mr. FRANK. I think obviously we can deal with deception under existing law. It's sometimes hard to prove. And children is obviously a separate case where they give up their own information, and you can say with regard to underage people they need protection.

I guess the thing we have to address is people who give information voluntarily, adults, for one purpose, and then find that it used for another. Is there any law on that or is that now wide open for people to do what they want?

Mr. MEDINE. Well again that's the issue of whether firms are voluntarily telling consumers how they're going to use the data. If they say we will use it to fulfill your order and for no other purpose, and they don't honor that, then that's deceptive.

Mr. FRANK. Most people don't think to ask.

I would ask for another couple of minutes, Mr. Chairman.

Mr. COBLE. Without objection.

Mr. FRANK. I think, you know, most of us when we're buying something don't stop and think to ask now what else are you going to use this for. I mean I agree if they tell you one thing and violate it that's a different story. And if they say to you, by the way, we're going to take this information and sell it to people who will forever after call you up at dinner time and harass you, then I might not buy it. So I think most of these fall into the category of people who get the information from you, and I think most people assume that it's only going to be for this purpose, but it's for another purpose. Is there any law in that area?

Mr. MEDINE. There isn't, and that's where we're looking for self-regulation. That's why we're surveying web sites to see what percentage are voluntarily providing consumers information about their practices, and again we will report to Congress on June 1st about that.

Mr. FRANK. Well let me ask you, I mean why shouldn't we do this self-regulation. If I'm self-regulating how is the law going to hurt me? The law doesn't hurt me if I'm self-regulating. It just tells me I should do what I'm already doing.

Mr. MEDINE. Well you'll have to take that up with industry. Our approach has been to try to——

Mr. FRANK. We'll have to take it up with who? With industry, no.

Mr. MEDINE. I mean our view has been let's give industry a chance to do all that voluntarily without the need for a law pressing them on that.

Mr. FRANK. Why? Excuse me, why? What is this, like law is some bad thing? You know, laws properly enforced don't walk around and bite people. If the law says you should not take information from people without telling them you're going to use it for another purpose and they use it for another purpose, who is that law hurting?

Mr. MEDINE. Well I think the concern has been that laws can somehow, depending on how they're drafted, confine the development of an industry, be technology specific and not allow for new technologies to be developed. There is tremendous change going on.

Mr. FRANK. Those are all those fake reasons I'm talking about. You know, they tell us that because they really want to keep going. By the way, I don't mean to get into a turf battle here, but they're more worried about how you enforce them than how we draft them has been my experience.

Let me just ask, finally, if there is a compendium, if anybody has done one and, if not, I would urge, Ambassador, and I think you're the highest ranking Executive Branch official here, could we ask for a kind of compendium on what the law now is maybe working interdepartmentally through Justice. I think it would be very helpful for this subcommittee. If by the end of this session for next year, and I mean I'm not looking for something instantly, but after we adjourn for the year and have gone home and we've stopped pestering you, if we could have an interdepartmental effort that laid out the state of the law on this subject matter I think that would be a very useful jumping off point for us for next year, Mr. Chairman.

I thank you for the extra time.

Mr. AARON. We would be happy to arrange that. OMB actually has prepared such a document a year ago, and we can make sure that it's updated.

Mr. FRANK. Yes, if they could because obviously things are changing and if it could be passed around. Do they get input from all the other departmental agencies?

Mr. AARON. Oh, yes.

Mr. FRANK. And I assume from the regulatory agencies as well.

Mr. AARON. They make sure that we are involved.

Mr. FRANK. Did they release that document? I don't know if we've seen it.

Mr. AARON. I'm sorry?

Mr. FRANK. Have they released that document?

Mr. AARON. Yes. I understand that was circulated a year ago or produced and made public a year ago.

Mr. FRANK. Made public a year ago.

Mr. AARON. Yes, and Justice was involved also.

Mr. COBLE. I thank the gentleman.

The gentleman from Virginia, Mr. Goodlatte is recognized for 5 minutes.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Ambassador Aaron, welcome. I would like to commend you on your efforts to promote electronic commerce and protect individual

privacy. It's something that is of great concern to me and I think vitally important to see the Internet reach its full potential.

As you know, I have introduced legislation that is designed to make sure that one of the primary tools for protecting privacy and promoting electronic commerce is available to all law-abiding citizens, and that is the use of strong encryption, and it would be my interest in hearing your comments on the efforts that have been pursued in the Congress and in the Administration to reach an agreement on the most effective way to do that.

I know that there are certain law enforcement concerns about encryption being used by those who are not law-abiding citizens who want to cover up their own activities, and the FBI and others have some concerns about that which I share with them. However, I do not share the solution that they have put forward which is to require every law-abiding citizen to put the key to their software programs in a location where law enforcement can access it without their knowledge.

This is a massive erosion of the Fourth Amendment privacy rights of United States citizens, and it would be exceedingly harmful to the software industry in the United States which would effectively have their packaging labeled with a different standard than the foreign competition that is out there in more than 20 countries around the world today. Ultimately the effect of that will be to stunt, as the current export control policy of the Administration is doing, the growing use of strong encryption in advancing the Internet for all means of electronic commerce, protecting credit cards, medical records, copyrighted material, industrial trade secrets and protecting the infrastructure of our country, whether it be the New York Stock Exchange or a nuclear power plant.

Encryption serves vital functions, and I'm concerned that this Administration's policy is retarding the growth and use of encryption, and that certainly is the consensus opinion of not only the software and hardware computer industries, but also of the business community in general because my legislation has been endorsed by the U.S. Chamber of Commerce, the National Association of Manufacturers and a number of other respected organizations that are concerned about having electronic commerce grow on the Internet.

Would you respond to that.

Mr. AARON. I think it's important to recognize that the Administration's encryption policy is not designed to require every American to place a key to their encryption in the hands of either the government or a third party.

Mr. GOODLATTE. But in order to get an export control license you have to come forward with a key recovery plan in order to export the product, and the Internet being an international function it is not feasible to have domestic encryption. There is no law against the domestic use of encryption today, you are correct about that. But if you're going to use something in your New York and San Francisco offices and also in your London, Paris and Tokyo offices you've got to be able to export that encryption in order to utilize it, and our policy seems to very much retard that.

Mr. AARON. The policy on export controls is designed to encourage the development and sale of key recoverable encryption around

the world, including in the United States. It does not require it. As you pointed out, there are no requirements within the United States that kind of encryption is to be used by American citizens. But the export controls do require that above a certain strength exported encryption software would be sold abroad, is required to have key recovery features at least by the end of this year, and for even stronger encryption it's required now.

Mr. GOODLATTE. Isn't that effectively mandating a key recovery system for the United States? It may not be the actual law, but the effect of having export controls is to create domestic controls.

Mr. AARON. I've always been a little baffled by that concern because we have the largest [by far] Internet computer information technology market in the world. Within the United States, we have a fair number of very powerful, in fact virtually unbreakable encryption programs that are for sale within the United States. I can't say, despite all the attention by industry, that the export control laws are what are holding back the promise of encryption.

I believe most people who have analyzed this with some expertise believe that what is holding back encryption and its more widespread use within the United States is in fact the absence of appropriate certificate authorities and authenticating bodies that enable people who are communicating with encrypted names from knowing who the person is they're communicating with.

Mr. GOODLATTE. Well that's obviously not the focus of the industry because they have placed great emphasis on changing the export control laws, and obviously they feel that they have been hindered in their ability to compete.

I'm also aware of the fact that you have been engaged in negotiations with other countries around the world in an effort to get them to adopt similar standards to those standards of the United States, not a market-driven policy, but a governmental policy, and it's my understanding that those efforts have been lacking in success, which indicates again to me that this policy of trying to use export control laws to guide the market with regard to the use of encryption is not going to work. It's failing.

Mr. AARON. I wouldn't agree with that assessment, Mr. Goodlatte. My experience in discussing these matters with foreign governments is that two things are underway. First of all, foreign governments are making their own policies, the Canadian Government, the Swedish Government, the British Government and the French Government. The French have made their policy, and the other three governments are in the process of making their policies. They are all trying to come to the same point that we're trying to reach here in the United States, which is how to balance the need for strong encryption against the requirements of law enforcement.

I think it's extremely important to recognize that if we go forward with technologies that do not permit law enforcement to continue to conduct electronic surveillance this will have a powerful impact on the ability of law enforcement to carry out its responsibilities. Understandably all markets are quite concerned about the impact on an enforcement, and every government is going through the same difficult task of balancing these issues. As you point out the law enforcement community does have a deep concern

here and their interests are quite different than that of the business community in some very specific sectors.

I think that there is a possibility (with good will on both sides) to find middle ground so that we can have strong encryption for all the purposes that are necessary to protect privacy and at the same time not give a blank check to criminal elements in our society.

Mr. GOODLATTE. Well, Ambassador Aaron, my time has expired.

Mr. Chairman, I would ask unanimous consent for a couple of additional minutes.

Mr. COBLE. Without objection.

Mr. GOODLATTE. I hope you are right about that. I share law enforcement's concern, as you say, but I do not share the solution that they have offered because I don't think it's workable. It is clear that those who are dedicated to acquiring encryption to misuse it already have access to it. The Cali Cartel is known to have software engineers who write and create encryption programs. You can download encryption off the Internet, and you can buy it from more than 20 foreign countries right now. You mentioned four that are in various stages of considering the issue, but there are nearly 200 nations around the world, and access to encryption for those who are bent on violating the law is very easy. It's not like your standard export control product, like a bomb or a jet or a mainframe computer where there are few manufacturers and there are a few known recipients of these, and the funnel through our export process can be fairly effective at restricting access to these things.

Here we're talking about an idea, mathematical algorithms, little 1's and 0's going through wires. Every day there are individuals who violate the export control laws of the United States without their knowledge by sending encrypted material between this country and other countries, and to use those laws for this purpose I think is totally ineffective. I think most other nations around the world are recognizing that.

Mr. Chairman, with your permission I would like submit for the record two articles from the *New York Times*, one dated October 9, 1997, which is entitled "Europeans Reject U.S. Plan on Electronic Cryptography," which talks about a meeting of the European Commission that had rejected the proposals by the United States aimed at ensuring that police agencies can crack coded messages over telephone and computer networks, and more recently a February 9, 1998 *New York Times* article entitled "Support for Encryption is Less than U.S. Claims Study Says," and it starts out "The Clinton Administration is losing its battle to increase international controls over how reliably computer data can be scrambled to ensure privacy according to reports scheduled to be released Monday by an independent research group."

This report goes on to quote individuals who say "I don't see any clear consensus out there in the world. I think the governments are equally divided on the issues and are not likely to try and follow the U.S. in trying to go down the path of the U.S. in the key recovery scheme."

Mr. Chairman, if these could be made a part of the record I would appreciate it.

Mr. COBLE. Without objection they will be indeed made a part of the record.

Mr. GOODLATTE. Thank you, Ambassador Aaron.
[The information referred to follows:]

CyberTimes The New York Times on the Web

Home | Site Index | Site Search | Forums | Archives | Marketplace

February 9, 1998

Support for Encryption Is Less Than U.S. Claims, Study Says

By JERI CLAUSING

WASHINGTON – The Clinton administration is losing its battle to increase international controls over how reliably computer data can be scrambled to insure privacy, according to a report scheduled to be released Monday by an independent research group.

The administration has been lobbying members of the European Union and other industrialized nations to back its efforts to place controls on "strong encryption," a technology for scrambling data so effectively that the code cannot be broken and the content cannot be deciphered without a digital key.

Data encrypting is used increasingly to protect the privacy of financial transactions, medical records and business communications. The administration wants the ability to descramble all encrypted messages to keep tabs on criminals.

The Encryption Debate:

Is It About Privacy or Security?

Go to Forum
Related Articles

In a report scheduled to be released Monday, the Electronic Privacy Information Center, a Washington-based research group, says that its survey of 243 governments showed that the United States is virtually the only democratic, industrialized nation seeking domestic regulation of strong encryption.

Today in CyberTimes

ARTICLES AND COLUMNS

Support for Encryption Is Less Than U.S. Claims, Study Says
By Jeri Clausing

Another Millennium Glitch Looks Weeks After Jan. 1
By Matthew L. Wald

Hollywood Pros Seek to Put Music, Movies and More on PC
By Andrew Pollack

AOL to Raise Prices 10%
By The Associated Press

A Maverick Builds a New Supercomputer in a PC World
By John Markoff

More Join Challenge to Library Over Blocking of Internet Sites
By The Associated Press

2 Internet Access Services Discuss Joining Forces
By Bloomberg News

High-Speed Fiber Optic Network Is Set for Los Angeles
By Reuters

E-Mail Alerts Show Growing Potential
By Bill Dedman

Want to Sell a Video Game? Better Stick With a Sports Theme
By Matt Richtel

Microsoft Case May Be Prelude to a Wider Antitrust Battle
By Steve Lohr

With Computers,

That finding directly contradicts the Clinton administration's assertion in congressional hearings that it has the support of most nations on this issue.

David Sobel, who directed the study by the research group for the Global Internet Liberty Campaign, a civil-liberties advocacy group, said of the administration: "They make the claim that other countries are accepting the U.S. position on this, then in an attempt to make that a reality, our government launched a worldwide lobbying campaign on encryption policy."

William Reinsch, the undersecretary for export administration in the U.S. Commerce Department, denied that the study contradicted the administration's assertions.

"All the administration has ever said is that there are more countries that go farther than we do," he said. "The study confirms that. And what I've gone on to say is that in talks with other countries, they are moving in our direction. I don't think the study itself does anything to contradict that."

The report comes as Congress prepares to renew what has become a contentious debate on encryption policy. Currently, the United States controls only the export of strong encryption. But the administration is pushing for a system that would give a third party a set of spare keys to all scrambled data so that law enforcement agencies could gain easy access to otherwise uncrackable computer files. The Federal Bureau of Investigation is pushing for a mandatory key recovery system that would guarantee the agency "immediate" access to the communications and data of suspected criminals.

Key recovery, as such systems are known, is opposed by virtually everyone outside of law enforcement agencies, including groups as diverse as the American Civil Liberties Union and the National Rifle Association. Opponents argue that such systems would be analogous to being required to leave copies of your letters at the post office in case some day you were suspected of committing a crime.

The survey, based on direct questioning of officials in more than 200 nations and territories, found that in the "vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction," according to the report.

"This is true for both leading industrial countries and for countries in emerging markets," the report says. "We also noted that recent trends in international law and policy suggest greater relaxation in controls on cryptography. There are a small number of countries

With Computers, Ugliness Overshadows Beauty
By Edward Rothstein

Museum Takes On a Science Project
By Pamela Mendels

Celebrating Black History Month
By Sreenath Sreenivasan

TODAY'S SECTION FRONT

SEVEN-DAY INDEX

CYBERTIMES FORUMS

CYBERTIMES NAVIGATOR

cryptography. There are a small number of countries where strong domestic controls on the use of cryptography are in place. These include Belarus, China, Israel, Pakistan, Russia, and Singapore. There are an even smaller number of countries that are currently considering the adoption of new controls. These include India, South Korea and the United States."

The report calls the policies of the United States "most surprising, given the fact that virtually all of the other democratic, industrial nations have few if any controls on the use of cryptography."

It goes on to obeserve that the administration's position "may be explained, in part, by the dominant role that state security agencies in the U.S. hold in the development of encryption policy."

France is a notable exception to the international trend, having one of the most restrictive encryption control policies in the world. But the movement there has been toward easing those controls, according to the report. Last August, Industry Minister Christian Pierret said that France would liberalize its encryption policies to "allow French companies to fully enter the market of electronic commerce currently dominated by U.S. companies."

Sobel said that the study was conducted, in part, "to test the administration's representations about the state of play around the world on this issues, because they have been pretty outspoken in congressional hearings in claiming that the U.S. policy is in line with what other governments are inclined to do with respect the encryption issues."

Reinsch defended those claims. "What we are finding in talks with government after government is a recognition of the need to create key management infrastructure," he said.

Lynn McNulty, a retired associated director for computer security at the National Institute for Standards and Technology who now is director of government affairs for the RSA Data Security, a developer of commercial encryption software, said he was not surprised by the survey's findings.

"I don't see any clear consensus out there in the world," McNulty said. "I think the governments are equally divided on this issues and are not likely to try and follow the U.S. in trying to go down the path of the U.S. in the key recovery scheme."

Related Sites

Following are links to the external Web sites mentioned in this article. These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability. When you have finished visiting any of these sites, you will be able to return to this page by clicking on your Web browser's "Back" button or icon until this page reappears.

- Electronic Privacy Information Center

CyberTimes

The New York Times on the Web

October 9, 1997

Europeans Reject U.S. Plan on Electronic Cryptography

By EDMUND L. ANDREWS

FRANKFURT -- The European Commission has rejected proposals by the United States aimed at insuring that police agencies can crack coded messages over telephone and computer networks.

In a lengthy report released Wednesday, the European Commission said the American approach could threaten privacy and stifle the growth of electronic commerce and that it might simply be ineffective.

RELATED ARTICLE
U.S. Official Says Clinton Wants Market-Driven Encryption Policy

The report appears to all but doom efforts by the Clinton Administration and the Federal Bureau of Investigation to establish a global system in which people who use cryptography would have to deposit a "key" for unlocking their codes with an independent outside organization. As envisioned, the police or intelligence agents would be able to use this key once they got court approval to carry out a wiretap. The plan has been vigorously opposed by the computer industry, which fears that it would jeopardize sales to foreign customers.

Because of the Internet's borderless nature, American officials have long acknowledged that their plan is workable only if most other countries adopt similar systems. If not, people could simply route their communications through countries with no restrictions.

The White House had already run into heavy opposition from civil rights groups, the computer industry and Congressional Republicans. And earlier this year, the United States failed to muster any support for its plan from the Organisation for Economic Co-operation and Development, a consortium backed by more than 40 countries.

But the European Commission's blunt opposition, reported Wednesday in The Wall Street Journal, went considerably further, raising a slew of objections to "key recovery" and "key escrow" systems. Among them were these:

- Hackers could find new ways to breach security. "Inevitably, any key access scheme introduces additional ways to break into a cryptographic system," the report said.
- The systems could weaken European data-privacy laws. "Any regulation hindering the use of encryption products," the report said, "hinders the secure and free flow of personal information."
- Even with a "key escrow" or "key recovery" system, criminals cannot be entirely prevented from using strong encryption.

More broadly, the European Commission said, any kind of key-based system could jeopardize the rise of electronic commerce.

"If citizens and companies have to fear that their communication and transactions are monitored with the help of key access or similar schemes," the report said, "they may prefer remaining in the anonymous off-line world."

American officials did not disguise their disappointment, and challenged the Europeans to come up with better alternatives.

"I am a little surprised," said William Reinsch, Deputy Secretary of Commerce in charge of export administration. "My question to the European Commission is, where do they think the market is going? Our sense is that corporations engaged in electronic commerce want key recovery in some form, because they want to recover their own records and to monitor their own employees."

The Encryption Debate:

Is It About Privacy or Security?

Go to Forum
Related Articles

Beyond high-minded policy issues, European officials quietly acknowledge that they have political and economic concerns. For one thing, several countries do not like the idea of deferring to an American system that might allow American companies to dominate the next generation of security products.

The German Government, meanwhile, is worried that American authorities might have improper access to data on German users -- possibly violating Germany's tough new laws on data protection.

But the European Union is far from united. Britain has generally sided with the United States in supporting an international system for regulating data **encryption**.

Indeed, the European Commission remained vague about what alternatives to the American system it might actually favor, nor does the report attempt to block member countries from setting up key-based systems if they want to.

American computer and software companies greeted the European policy declaration as a victory.

"Even the hard-line Governments, the U.S. and the United Kingdom, have said that any cryptography restrictions have to be internationally coordinated because otherwise you can just download material from another country," said Chris Kuner, a lawyer in Frankfurt who represents Netscape Communications and other networking companies in Europe.

"This shows that Europe does not agree with the idea of mandatory key recovery. This idea that that is the only possible regulatory framework for the world has been clearly rejected."

Mr. COBLE. The gentleman's time has expired.

The gentleman from Massachusetts, Mr. Delahunt.

Mr. FRANK. Mr. Chairman, if I could just briefly. I did want to make clear, as people are looking at the witnesses and might have a question, that my staff did call some of the business enterprises that are in the business of buying and selling some of this information, and they declined to comment. So I did want to say we did ask some of those whose business practices we are implicitly criticizing to come, and as of now they decided they didn't want to. So if there is a one sidedness there we did try to avoid that.

Mr. COBLE. So noted.

The gentleman from Massachusetts, Mr. Delahunt is recognized for 5 minutes.

Mr. DELAHUNT. Thank you, Mr. Chairman.

I think I would like to give Ambassador Aaron an opportunity to respond to my colleague from Virginia's remarks and observations. I should also add that I share in many respects those observations just made by Representative Goodlatte.

Mr. AARON. Thank you very much. I appreciate the opportunity to do so. I think it is a false distinction to say that if you cannot have perfection in controlling encryption you shouldn't do it at all. I don't think our law enforcement authorities believe that they're going to keep encryption out of the hands of the most sophisticated terrorists and criminals like the Cali Cartel, but there is a world of difference between this and a situation where common people have access to secure communications. They've had access to secure communications for decades. They've had safe houses and couriers and other means to communicate. But that's a world of difference between every malcontent, every would-be terrorist bomb-maker, every common criminal, every drug-pusher hanging around on the corner and——

Mr. DELAHUNT. I think that——

Mr. AARON. May I please complete my comment.

Mr. DELAHUNT. Sure.

Mr. AARON. It's a world of difference when all of them are crypto geniuses by just pushing a button on either a computer or a telephone. I think that this is the nightmare that the FBI faces, and this is a fundamental decision that perhaps the Congress is going to have to make. We will have to decide whether we are going to allow the FBI to no longer have any ability to intercept communications or for that matter to recover stored data in files that's encrypted. Are we going to say they're just going to have to live with that kind of constraint? And if our decision is that, no, that isn't the right thing to do, then we've got to find an answer. Now the Administration has proposed an answer. Industry, I might add, despite the expressions of sympathy for this situation, has not proposed an answer.

So, again, I'm pleading here for a little effort to find common ground. I'm just deeply distressed that the issue is so terribly polarized, and I don't think it's very helpful to our national security, nor the advance of our industry, to have each side completely rejecting the interests of the other.

I guess my plea here would be if we're going to have a real discussion about encryption on the Hill that we try to do it from the

standpoint of really trying to serve both interests. They are very difficult to reconcile, but in my judgment it's a reconciliation that really needs to take place.

Mr. DELAHUNT. Again, with all due respect, Ambassador, I have, you know, listened and heard my colleague from Virginia address this issue, and I for one feel strongly that he has made a prodigious effort to find the middle ground, if you will. I don't know what the status of his efforts are at this particular point in time, but I think, and this is the concern that I share, that in the real world today you have the ability to have such ready access to any kind of encryption. Again he made reference to the fact that it could be just simply downloaded on the Internet and end up in the hands of a terrorist from any part of the world. You know, simply getting on a plane and arriving in New York and going to Computer World, where it's on shelf and have the availability there and getting back on the plane. I mean this is how someone who if they are dedicated and intent on acquiring that technology, it is so readily available that our policy right now I don't think in any way deters that kind of an individual, that kind of organization from securing it.

Mr. AARON. I agree with you.

Mr. DELAHUNT. That's the problem.

Mr. AARON. No, I agree with you, and I don't think there is a solution for that kind of situation.

Mr. DELAHUNT. But what we do simultaneously is hurt our own——

Mr. AARON. I don't think that's the issue that law enforcement is concerned about. I think the issue that law enforcement is concerned about is to have it in the hands of virtually anybody who has some malevolent designs and who is not a crypto genius and who doesn't have the resources to go to this place and that place.

I'm struck by the fact that we are constantly talking about how cryptography is so readily available, but the fact of the matter is it really isn't that widely used. Now there are reasons for that, and it's not export controls. The reason is that it's not very user friendly. We've heard for three or 4 years that the horse is out of the barn. Well the best that I could say from having worked on this now for more than a year is that I don't even think the beta version of the horse is out of the barn. I think that you have some encryption out there that is not saleable, you cannot use it widely, it's not user friendly, you can't just attach it to your phone, and you can't just put it into your computer and then communicate with anybody in the world in an encrypted way. You can't do that. The systems really don't exist yet. We still have time to try to reach a decision whether anybody who has criminal interests is going to be able to use this with no possibility of law enforcement ever having any access to it.

I cannot stress enough that the reason law enforcement officials are so concerned about this is not because they're blind or don't understand or don't get it. They get it fine. They get the fact that the interception of communications under court order and the ability to seize files and read them under court order is vital to their law enforcement function, and they see the possibility that this technology will make that impossible.

We really need to think through if we're going to go down the road of saying, "well it's just too hard, it's too difficult because it's too important to industry, so therefore let's just have strong encryption for everybody," and we'll just leave it at that. We will really have to think through how our law enforcement in this country, and for that matter in the world, is going to function because it's going to be a very difficult proposition. And if we haven't thought that through, then maybe we ought to just take a little time to see if there isn't some compromise that's possible between the interests of law enforcement and industry.

Mr. DELAHUNT. Mr. Chairman, my time has expired. Thank you.

Mr. COBLE. If you have another question go ahead.

Mr. DELAHUNT. I do have several other questions.

Mr. COBLE. We'll do this family style this morning and give a long leash on time.

Mr. DELAHUNT. Well I'll be brief in those.

You know, we're talking again about self-regulation and the current status of the law, and I guess I would direct this to Mr. Medine and also to Ambassador Aaron. What kind of complaints are you getting? I mean what is the extent—has there been any analysis or review—of the problem? I mean there is a problem presumably because we're here, but what is the extent of it, and why don't you provide us with any empirical data that you might have available and an anecdote or two if you can do it concisely.

Mr. MEDINE. Actually what I think is unique about this hearing and unique about the Federal Trade Commission's efforts in this area has been that we've been acting before a problem arises to try to address consumer concerns in advance. We're trying to create a marketplace where consumers have confidence and are interested in shopping. So we don't have the horror stories yet, and that gives us the opportunity, as new systems are being developed to integrate privacy protection before those horror stories occur and we have to just respond to those accounts.

What we do have is survey data that shows that consumers are very concerned, increasingly concerned about their privacy online, that they are staying away from this marketplace, and that's a significant trend because if consumers stay away, this marketplace will not develop and reach its full potential. So what we're trying to do is to encourage an awareness of this issue with industry members so that they can respond voluntarily.

Mr. DELAHUNT. So you're saying there is no measurable problem at this point in time?

Mr. MEDINE. I think that's basically right because, first of all, consumers oftentimes don't know if their privacy has been invaded because they don't know some of the subsequent uses of their data.

Mr. DELAHUNT. Given the question posed by Mr. Frank in terms of information being provided unbeknownst to the consumer.

Mr. MEDINE. That's right, they may not know. If they get a catalog in the mail or if they get contacted they may not know.

Mr. DELAHUNT. What prompted, and I think you made reference to a group that has applied these IRSG principles, 14 companies and 3 credit card companies that are sitting down trying to work out a protocol, if you will.

Mr. MEDINE. What prompted that was an incident involving a service called Lexus-P-Trak which came to attention——

Mr. DELAHUNT. We're starting to get into the problems now, but go ahead.

Mr. MEDINE [continuing]. Which first came to attention on the Internet as being a database that consumers were unaware of, not that there were necessarily identifiable problems so much as there was consumer concern that there was information about them available that they were not even aware existed, and databases exchanging that information, and that concern went to the media and then to Congress, and Congress asked us to take a very close look at this industry.

Mr. FRANK. Would the gentleman yield?

Mr. DELAHUNT. I'll yield.

Mr. FRANK. Was that the one with the Social Security numbers?

Mr. MEDINE. Yes.

Mr. FRANK. People's Social Security numbers showing up.

Mr. MEDINE. Yes, Social Security numbers, mother's maiden name was at least alleged, and actually it turned out to be just your maiden name, and information about birth and location. Social Security numbers were certainly a primary motivation for that, and again that's why we were asked to do it. There are cases of identity theft, and they're very hard to tie in, a case of identity theft from the source of that information. So again it's hard sometimes to tie in the injury to the invasion of privacy.

Mr. DELAHUNT. At this point in time there is nothing, or is there, to prevent the exchange of this kind information other than industry private sector self-regulation?

Mr. MEDINE. That is by and large the case. The way we look at it is that we have experience with the credit card market, and that's a situation that in 1968 and 1970 Congress enacted some protections for consumers on the use of credit cards, liability limits and billing dispute procedures, and that created a consumer confidence in the industry that allowed the credit card market to take off dramatically. By contrast the 900 number——

Mr. DELAHUNT. Now we have three billion solicitations annually.

Mr. MEDINE. Well, the contrast is the 900 number industry which started off very strong and was beset by fraud and sales feel off dramatically because consumers lost confidence in that medium. We all carry credit cards in our wallet today and walk down the street because we have those Congressionally mandated protections. Now the protections can come either from Congress or from the industry, but consumers need confidence in a marketplace for it to take off. We're really at the crossroads now of electronic commerce taking off or not, and we think privacy protections are integral to that.

Mr. DELAHUNT. This will be my last question, Mr. Chairman, and I thank you for indulging me.

Within your purview and your statutory authority the penalties or the sanctions that are available are all civil in nature. You would obviously have to refer I presume any criminal activity you discovered to the Department of Justice; is that correct?

Mr. MEDINE. That's absolutely correct.

Mr. DELAHUNT. How many referrals in this whole privacy area have you made, if you have an idea?

Mr. MEDINE. Well, again, our statutory authority is limited in the area of criminal sanctions. This area is limited. There have been a few instances in the Fair Credit Reporting context in which we have made criminal referrals to the Justice Department, and that is the place where we would make referrals because we lack criminal prosecution authority, but we would work with the Department or the U.S. Attorney's Office in prosecuting in that instance.

Mr. DELAHUNT. In those really egregious cases I sense there is no deterrence out there whatsoever at this point in time because, you know, if you get away with it, fine. I mean so there is some sort of an injunction against unfair practices. Well, you know, who cares?

Mr. MEDINE. Well we think that firms do pay attention to both the publicity associated with enforcement actions and to the fact that they would be subject to criminal or civil contempt for violations of our orders, and there are provisions for providing redress and restitution. So there are a range of remedies that are available to us that I think can keep firms' privacy practices in line.

Mr. DELAHUNT. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

The gentleman from California, Mr. Rogan.

Mr. ROGAN. Thank you, Mr. Chairman, for calling this hearing. I thank Mr. Medine and Ambassador Aaron for joining us today.

I appreciate your respective comments in your prepared and in your presented testimony relating to private efforts of industry being preferable to government regulation. I applaud that sentiment.

I'm especially mindful of what Ambassador Aaron talked about a few minutes ago when he spoke of the need to balance strong encryption against the needs of law enforcement. I think that dovetails on what Mr. Medine said. Mr. Medine is absolutely right when he said that we are at a crossroads as to whether electronic commerce will really take off, and privacy concerns are integral to it.

I don't want to turn this into a subcommittee hearing on encryption, but having listened to the comments here today from my colleague from Virginia, and mindful of our previous debate in the House, I can't help but think that there are a lot of other instances where that balancing act between the needs of law enforcement and an individual's right of privacy come into play.

Thus, this balance relative to encryption is not a unique circumstance. For instance, if two conspirators are walking down the street together and suddenly duck into a restaurant and go into a back room and have a conspiratorial conversation, I imagine that any law enforcement official would like to be able to tap into that conversation and be able to act upon it. But barring their foresight to have a bug planted in that room or some ability to electronically eavesdrop at the last moment there are just times when that desire is not available to act upon. There are remedies, of course. We could simply outlaw the concept of people walking down the street and ducking into a restaurant to talk; we could just bug every back

room and every table. But in the interest of liberty, we make a judgment call that such laws would not be appropriate. In fact, procedurally we place a number of obstacles before law enforcement officials wishing to eavesdrop.

I only raise this issue because in reviewing Ambassador Aaron's testimony, he presents many hopeful aspects, but the prospect for a hammer certainly is present. On the last page, quoting from the Ambassador's prepared testimony he said "We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation. But if effective privacy protection cannot be provided in this way, we will reevaluate this policy." I know that based on your testimony that on July 1st a report is going to be prepared for the President relating to this subject.

Ambassador Aaron, or Mr. Medine, do you have any preliminary observations as to how industry might be faring in this regard prior to the publication of the July 1st report?

Mr. AARON. Yes, I think I can comment at least in part on that. Let me just say in response to some of the earlier discussion here that we have never felt that self-regulation was the only tool for ensuring privacy. It's our feeling that it really has to be a combination of measures that includes law, includes regulation and includes self-regulation where it is more appropriate, efficient or cost-effective.

Mr. ROGAN. If I may interrupt just for a moment so I may follow you. Certainly the assumption in that comment is that if the standard that the Administration might like to see is not met, the other side of the scale begins to tip higher.

Mr. AARON. Well I wouldn't put it in those terms, but I would say that different circumstances require different measures. For example, we have seen the validity and importance of law and regulation in certain sectors. As I indicated earlier, the sectors include telecommunications, medical information and genetic information, financial sector, and so forth. I just want to make it clear that we're not just saying that self-regulation is the only answer.

It's really our judgment that the Internet, because it is so rapidly evolving and so multifaceted, that it is best to try to get the industry itself to embark on self-regulation. So far, to be frank, we are off to a slow start, but I think there is hope. There are some leading companies who are seeking to bring together other companies to adopt self-regulatory regimes that would be consistent with the kinds of criteria which I enunciated in my presentation, and we believe that by July 1 we should be in a position to report some substantial progress in that area.

I don't want to identify the companies. I want to let them go ahead and do their work. I think the picture is reasonable encouraging at this point, but it has take significant encouragement on the part of Secretary Daley and others to get to this point and we're going to need to continue that dialogue with industry.

I believe the Department has two different activities coming up. In May, the Department of Commerce is going to have a 2-day conference with industry, consumer groups and government officials to look at the issue of self-regulation and its enforcement and how effective it can be in protecting privacy. We will follow up that con-

ference with meetings with industry and consumer groups in a variety of fashions prior to the July 1 deadline.

But as you point out, and I'm sorry I didn't get to that point because my little red light had gone on, the Administration does believe that private efforts of industry working in cooperation with consumer groups can be more effective and are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.

Mr. ROGAN. Mr. Chairman, I see that my time has expired.

Mr. COBLE. Well if you have another question or two you are welcome to ask them. We're informal this morning.

Mr. ROGAN. Actually I had promised my friend from Virginia I would yield a minute to him. So I wonder if the committee would indulge me so as not to make a liar out of me in his eyes.

Mr. COBLE. Without objection.

Mr. ROGAN. I yield to my colleague from Virginia.

Mr. GOODLATTE. I thank the gentleman for yielding, and I also thank the gentleman from Massachusetts for his comments. He is one of a number of former prosecutors who recognized the difficulty that law enforcement has in dealing with encryption as I do, but nonetheless understands the nature of this problem and that the solution is not to keep encryption out of the hands of the good guys who can use it to protect themselves.

Ambassador Aaron, I just wanted to respond to a comment you made earlier asking if we wanted to have a situation where the FBI would no longer be able to use certain law enforcement techniques because of the existence of encryption, and I just want to dispute that. There is absolutely no question but that through both technological means and traditional law enforcement means there are a lot of other ways for law enforcement to address this problem. Will strong encryption be a problem for them? Absolutely. Whether my bill passes or not, it will be a significant problem for them, but they have the opportunity to work with the computer industry.

One of the provisions that was put into this legislation and one of the committees that dealt with it was a center for law enforcement to work with the high-tech industry to come up with a means of looking at this. This is not new either. Certain aspects of the law enforcement and intelligence communities have always engaged in that sort of activity to try to find the weak points in mathematical algorithms and use that. In addition, you have the opportunity to have undercover operations where somebody is given the key to the encryption by getting inside of an organization. Sometimes people inadvertently give the key out to other people.

You correctly noted that one of the problems in this whole area is the certificates of authority. How do you know whether the person you are communicating with is the person you think you're communicating with. There are a number of tools that law enforcement will have and will continue to use to deal with their lawful right under certain circumstances to intercept and decode communications.

So I don't want this issue to be at all polarized, and we are willing to look at a lot of different alternatives, but if one of those alternatives is the government mandating or even indirectly requiring certain activity of citizens that results in mandating, which is

what I believe our current export control laws effectively do, or having a key system where the gentleman from California correctly noted is the equivalent of the Congress requiring people to take the key to their home or their safe deposit box down to the police station and put it on deposit so that under certain circumstances the police can use it and come into their homes without their knowledge, that is a massive erosion of our Fourth Amendment rights and that's what we object to. Short of that there are a lot of things we can do and a lot of things we can and will in this legislation give to law enforcement to deal with the problem of encryption.

I thank the gentleman for yielding.

Mr. COBLE. I thank the gentleman.

The gentleman from Indiana, Mr. Pease.

Mr. PEASE. I thank the chairman and the members of the panel for being with us on this important subject, and I express my regret to the chairman and the members of the panel that multiple simultaneous duties have had me moving in and out, and because of that I think it's more appropriate that I waive my opportunity to question.

I do appreciate the written material and having reviewed it will probably be in touch, but thank you very much for your presentations.

Mr. COBLE. I thank the gentleman.

Gentlemen, we appreciate you being here. We may be in touch with you subsequently.

Now I may pay the price for having been so liberal on our time with the first panel because we're going to have a vote fairly imminently and I would like to be able to move this along. So I would ask the second panel if you all would adhere to the red light when it appears as your warning that the 5 minutes have elapsed.

Our first witness on the second panel is Fred Cate, who is a professor of law and Director of the Information Law and Commerce Institute at the Indiana University School of Law. Professor Cate is a recognized expert on information law and also the author of many articles addressing privacy, copyright and freedom of expression.

Our second witness is Mr. Marc Rotenberg, Director of the Electronic Privacy Information Center, a public interest research organization working to protect privacy, free speech and Constitutional values in the online world. Mr. Rotenberg is also an adjunct professor at Georgetown University Law Center.

Our third witness is Ms. Deirdre Mulligan. She is Staff Counsel at the Center for Democracy and Technology where she evaluates the impact of technology on individual privacy. Currently Ms. Mulligan is shepherding the Internet Privacy Working Group, a collaborative public interest/private sector working group, developing a framework for privacy on the Internet.

We had a fourth witness who because of personal problems could not appear, Ginlauri Goldman, who is the Director of Health Privacy Project at the Georgetown University Medical Center, and I would ask unanimous consent that her statement be made a part of the record as well as the statements of the members of the second panel.

Now, Professor Cate, we have a valued member of this subcommittee who is an alumnus of your School of Law, but I believe you look too young to have taught him. [Laughter.]

Am I correct about that?

Mr. CATE. Thank you very much, Mr. Chairman. I doubt if I could have taught the Member from Indiana anything at all.

Mr. FRANK. I had one other acknowledgement, Mr. Chairman. In the interests of full disclosure I should note that one of the witnesses has a connection. My first political event was held in his home. He was at the time I think about six. [Laughter.]

It was in 1972. Mr. Rotenberg's parents held my first political event in 1972. So I thought we should put that in the record. I do think he was probably of an age where he was certainly eligible to give personal information to various computer-generated businesses, but he was not himself I think a participant in the decision to host me, although I hope it is one he never later regretted.

Mr. COBLE. Mr. Rotenberg, we will hold you harmless for your past sins. That is said in jest of course. [Laughter.]

And I need to tell the gentleman from Indiana that I did not mean to imply that you looked that old, Mr. Pease. [Laughter.]

I'm getting in trouble. So having said that, Ms. Mulligan, why don't we start with you. And, again, folks, if you all could be ever mindful of the 5 minute time limit we will be appreciative.

STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MULLIGAN. Thank you very much. It's a pleasure to be here this morning to talk about this important issue.

While my mind and my nose were buried yesterday trying to finish my testimony, I neglected to read the Style Section of the Washington Post which I know is where most people start. As I was sitting around the living room last night with my friends and neighbors we started discussing the fact that, Kenneth Starr, went down to Kramer Books, and subpoenaed records of Monica Lewinsky's book purchases. I believe this is a good place to start my testimony.

We have entered a "Brave New World." It's a world in which our words are not the only important records, but in fact data itself speaks. And the little pieces of data that we leave in our daily transactions, whether they're with the book store or they're with an online service provider or they're with a web site, can come back and bite us.

When Kenneth Starr goes and asks Kramer Books for records of Monica Lewinsky's purchases at the book store we must think about the information he may find. Will he find that Monica was perhaps fighting depression? Will he find that she was curious about a particular health ailment in her family? What may be revealed by the records of her book purchases?

Historically the actions of data collectors in the private sector were rarely the focus of our privacy policies. Generally they have focused on law enforcement access. This case highlights that the wall between the private sector collection and use of data and the government's use of data when it decides to bring its force and actions into this world in the area of privacy is a permeable one. I'm

very pleased that the committee has decided to focus on the important issue of privacy in the electronic medium.

Perhaps the next type of information that Kenneth Starr will seek will be information from a cellular phone company, which in fact might be able to a year or so down the line detail not only whether Monica was in the White House, but what part of town she was in, and perhaps next year it would be able to tell us which room Monica visited in the White House. Because in fact that is the type of detailed transactional data that this digital revolution in technology is bringing upon us.

Crafting proper privacy protections in the electronic realm has always been a very complex endeavor. It requires a keen awareness not only of changes in technology, but also changes in how that technology is entering our daily lives.

The last time that Congress revisited this issue seriously was in 1986. Due to privacy considerations arising from changes in technology, primarily wireless services and the growing use of e-mail, Congress adopted the Electronic Communications Privacy Act. ECPA began to grapple at the edges of this revolution in communications and computing medium. It started to realize that this transactional data, not necessarily the words we speak, but the digital fingerprints that we leave as we walk through this world were beginning to talk very loudly about our thoughts, our associations, our whereabouts and our acquaintances.

I would like to use two brief examples to talk about what that might mean in the future and why I think that these changes in both technology and the way in which this technology is being embedded in the fabric of our lives requires us to reexamine how we craft privacy policies, how we deal with privacy institutionally within the government, and how to move forward.

Individuals traditionally kept their diaries under their bed, in their drawer or perhaps on their desk. With the advent of digital desktop computing people began to store their diaries on their hard drives. As network computing, which is where we are today, continues to become more and more an integral part of our lives those intimate papers, those thoughts and reflections are actually moving out into remote locations. What this means is that rather than having the full Fourth Amendment protections when law enforcement comes to seize my diary they would if they were stored in the home, they might be able to access that information under a much weaker legal standard—perhaps a mere subpoena if that record was kept on a remote server somewhere. That diary is still my diary regardless of where it is. Yet the legal protections afforded it might be quite different.

This becomes I think perhaps even more troubling to individuals if we think about some of the sensitive records that are held by institutions. Congress is focusing specifically on the privacy protections afforded medical records. It is an area on which we need to focus. Hospitals, clinics and physicians are using network computing in their businesses, and as those personal records that reveal the most intimate pieces of our lives go from the doctor's file to the doctor's desktop to a shared computing environment where they are no longer under the purview of the doctor—forget about my

right to have notice before those records are accessed—but in fact the doctor might not even realize when those records are accessed.

To conclude, in thinking about electronic communications as we move forward I would ask that Congress, one, reexamine the need for limits on the disclosure and use of personal information by private entities. This is a very important area that is in need of further thought. Reconsider how the lines have been drawn between records that are entitled to the full Fourth Amendment protection, such as my diary in my home, and the records that are considered business records, such as the records that Kenneth Starr subpoenaed from Kramer Books about Monica Lewinsky's First Amendment activities. It is time to heighten the standard for access to transactional data because it does reveal much more than just the phone numbers that we've dialed.

Finally, I would ask that you consider creating a privacy entity to deal with privacy policy as we move forward. It's going to continue to be a perplexing issue. Encryption has focused us on privacy. There will always be needs that people think outweigh Americans' interest in privacy, and we must have a cohesive body of thought and a place to develop institutional policies on this issue.

And, finally, I think that the government has——

Mr. COBLE. Ms. Mulligan, if you could wrap it up as soon as you can. I don't want to cut you off.

Ms. MULLIGAN. Yes, this is the last one. Technology does play an important role in protecting privacy and as many members of the subcommittee have stated this morning, encryption is one of those core technologies. I think your support for strong encryption in this coming age is of utmost importance. Thank you.

Mr. COBLE. Thank you.

[The prepared statement of Deirdre Mulligan follows:]

PREPARED STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

SUMMARY

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values in new digital media. One of our core goals is to enhance privacy protections for individuals in the development and use of new technologies.

It is critically important to ensure that privacy protections keep pace with changes in technology. This requires a periodic assessment of whether changes in technology pose new threats to privacy that must be addressed through changes in law. Many of our existing laws were constructed to meet dual purposes, such as protecting privacy and meeting legitimate law enforcement needs, or protecting privacy and promoting the cost effective operation of the health care system, the rules continue to set the bounds of permissible government action. We must examine whether they continue to do so in a fashion consistent with privacy protection. In addition, it requires us to evaluate whether technology itself can be used to advance privacy in this new environment. Finally, the globalization of the communications system requires us to consider alternative methods for achieving policy goals, be they self-regulation or international agreements. In other words, examining privacy protections in the changing electronic communications environment requires us to look freshly at old law, consider the creation of new law, consider the role of technology in promoting privacy, and explore new avenues of making policy.

Shifts in Technology

Several trends in technology have ramifications for the existing framework of privacy protections in electronic communications: the explosive growth of the Internet; the increase in transactional data generated; the globalization of communications

technology; the lack of centralized control mechanisms; and, the decrease in computing costs and the focus on client-side controls over network interactions.

Gaps in the legal framework

The current legal framework of Title III and ECPA did not envision the World Wide Web and the pervasive role technology would play in our daily lives. Underlying Title III and ECPA were a number of assumptions about both the nature and the use of electronic communications. While these assumptions may have been accurate at one point in history, communications technology and individuals' use of it have both changed dramatically since the initial framework for protecting electronic communications was articulated in 1968. The shift toward distributed networks and the proliferation of digital communications technology in our everyday interactions creates some interesting privacy consequences under the existing framework.

Conclusion and Recommendations

As we consider privacy in the changing communications environment we must ask whether policies designed to implement the Fourth Amendment developed in a 20th century world of paper records—even as extended to protect transient voice communications—are applicable to 21st century technologies where many of our most important records are not "papers" in our "houses" but "bytes" stored electronically and our communications rather than disappearing into thin air are captured and stored at distant "virtual" locations for indefinite periods of time.

To address privacy in the electronic communications environment the U.S. government should:

- Reexamine the need for limits on the disclosure and use of personal information by private entities.
- Reconsider how the lines have been drawn between records entitled to full Fourth Amendment protection and records under Miller that fall outside the protection of the Fourth Amendment.
- Heighten the standard for access to transactional data.
- Create a privacy protection entity to provide expertise and institutional memory, a forum for privacy research, exploration, and guidance, and a source of policy recommendations on privacy issues.
- Encourage the development and implementation of technologies that support privacy on global information networks.

STATEMENT

I. Introduction and Summary

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify on the issue of privacy protection in the online environment.

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

To focus my testimony this morning, I will begin by outlining five trends in technology with ramifications for the existing framework of privacy protections in electronic communications. The current mix of legal and self-regulatory protections for privacy has not kept pace with technology and its growing role in society. The core of my testimony is a series of policy recommendations:

- identifying areas in which Congress should enhance existing privacy protections;
- recommending the creation of an institutional structure for addressing privacy concerns in a proactive and ongoing manner; and,
- urging the US government (and others) to engage in several non-traditional methods of developing and implementing privacy policy that are of particular relevance to the global, decentralized networks that comprise our communications infrastructure.

It is critically important to ensure that privacy protections keep pace with changes in technology. This requires a periodic assessment of whether changes in technology pose new threats to privacy that must be addressed through changes in law. Many of our existing laws were constructed to meet dual purposes, such as protecting privacy and meeting legitimate law enforcement needs, or protecting privacy and promoting the cost-effective operation of the health care system. We must examine whether they continue to set the bounds of permissible government and private sec-

tor action in a fashion consistent with privacy protection. In addition, we should evaluate whether technology itself can be used to advance privacy in this new environment. Finally, the globalization of the communications system requires us to consider alternative methods for achieving policy goals, be they self-regulation or international agreements.

II. Technology trends with ramifications for individual privacy in electronic communications

A. The explosive growth of the Internet is transforming our methods of communicating and methods of gathering, processing and sharing information and knowledge. In 1986, when Congress updated the communications privacy laws,[1] the Internet was comprised of approximately 50,000 computers. Today the Internet is comprised of upwards of 20 million Internet host computers globally and estimates on individual users hover around 100 million people worldwide. Unlike traditional media, the Internet supports interactions ranging from banking to dating, from one to one communications, town hall meetings, political events, to commercial transactions.

B. The transactional data generated through the use of new technologies is a rich source of information about individuals' habits of association, speech, and commercial activities. This vast new data is essential to the operation of the packet-switching medium and provides the raw material for many of the unique functions the Internet offers, yet it poses significant privacy concerns. Interactive media generate, capture and store a tremendous amount of information. At the same time the flexibility of new media is blurring the distinction between the content of a communication and the transactional data used to route the message to its destination. Transactional data in this new media is more detailed, descriptive, and identifying than ever before. Aggregated, it is capable of revealing as much about the individual as the content of a message.

C. The globalization of communications technology is eroding national borders. Governments are finding it increasingly difficult to enforce laws—be they laws to protect or repress their citizens. The fluidity of borders on the Internet promises to promote pluralism, the free flow of information and ideas, diverse associations, and, we hope, democracy. On the other hand, enforceable, workable privacy protections for the global information infrastructure have yet to emerge leaving individuals' communications and personal data vulnerable.

D. The lack of centralized control mechanisms. The distributed nature of the Internet's infrastructure distinguishes it, at least in degree, from existing communications systems. Its decentralized nature allows it to cope with problems and failures in any given computer network by simply routing information along alternate paths. This makes the Internet quite robust. However, the lack of centralized control mechanisms may frustrate those seeking to regulate activities on the network.[2] Decentralized systems are inherently less secure. They pose new challenges to protecting data during storage and transmission.

E. Decrease in computing costs and the focus on client-side controls over network interactions present new opportunities to empower individuals. The Internet continues to shift control over interactions away from the government and large private sector companies. The ability to build privacy protections into the users interface with the network offers the opportunity to craft privacy protections that shield individuals regardless of the jurisdictional law and policy. Providing individuals with technical means to control and secure their communications and personal information may pave the way for privacy protections that are as decentralized and ubiquitous as the networks themselves.

III. Policies from the pre-network world

Current policies protecting individual privacy in electronic communications are built upon Fourth Amendment principles designed to protect citizens from government intrusion. While premised on Fourth Amendment concepts, the contours of existing statutory protections are also a product of the technical and social "givens" of specific moments in history. Some of these historical givens have changed dramatically, with implications for the effectiveness and relevance of existing statutory protections for privacy.

---

[1] Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§2510–21, 2701–10, 3121–26.

[2] Attempts to regulate the availability of encryption on the Internet highlight the frustrations that regulators may experience. As many scholars and advocates have pointed out, national attempts to restrict the availability of encryption are likely to be ineffective. For if even one jurisdiction (or one network in one jurisdiction) fails to restrict it, individuals world-wide will be able to access it over the Internet and use it.

Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how the technology is used by citizens, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. The issues raised below indicate that it is time for such a review.

A. From phones to email: The existing framework

In response to Supreme Court decisions finding that electronic surveillance was a search and seizure covered by the 4th Amendment[3] and law enforcement's arguments that it was a needed weapon against organized crime,[4] Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[5] The wiretap provisions of Title III authorized law enforcement wiretapping of telephones within a framework designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance.[6]

In brief, the legislation Congress enacted in 1968 had the following components: the content of wire communications could be seized by the government in criminal cases pursuant to a court order issued upon a finding of probable cause;[7] wiretapping would be otherwise outlawed;[8] wiretapping would be permitted only for specified crimes;[9] it would be authorized only as a last resort, when other investigative techniques would not work;[10] surveillance would be carried out in such a way as to "minimize" the interception of innocent conversations;[11] notice would be provided after the investigation had been concluded;[12] and there would be an opportunity prior to introduction of the evidence at any trial for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap.[13] "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime. The showing of a special need, in the form of a lack of other reasonable means to obtain the information, was viewed as justification for the failure to provide advance or contemporaneous notice of the search.[14]

Due to privacy considerations arising from changes in technology, primarily the advent of wireless services and the growing use of email, in 1986 Congress adopted the Electronic Communications Privacy Act (ECPA).[15] Congress' action was in part spurred by the recognition that individuals would be reluctant to use new technologies unless privacy protections were in place.[16]

ECPA did recognize the importance of transactional data. ECPA set forth rules for the use of pen registers and trap and trace devices, which capture out-going and incoming phone numbers respectively.[17] It also established rules for law enforcement access to information identifying subscribers of electronic communication services.[18] For transactional information relating to e-mail ECPA requires a warrant, for other transactional data it requires a court order, a mere subpoena, or consent.

To a large degree ECPA extended the Title III protections to the interception of wireless voice communications and to non-voice electronic communications such as

---

[3] *See* Berger v. New York, 388 U.S. 41, 56 (1967); Katz v. United States, 389 U.S. 347 (1967).

[4] *See Controlling Crime Through More Effective Law Enforcement: Hearings on S. 300, S. 552, S. 580, S. 674, S. 675, S. 678, S. 798, S. 824, S. 916, S. 917, S. 992, S. 1007, S. 1094, S. 1194, S. 1333, and S. 2050 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 90th Cong. (1967), passim.

[5] 18 U.S.C. §§2510–22 (1996).

[6] In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to regulate wiretapping in national security cases. It provides more limited protections than those afforded under Title III, and was meant to be used primarily in foreign intelligence and counter-intelligence cases. Of importance, FISA does not require that the subject of the surveillance ever be given notice, and for individuals who are not U.S. citizens or permanent residents it does not require the government to show probable cause that the target is engaged in criminal conduct. Pub. L. No. 95–511, tit. I, §101, 92 Stat. 1783 (1983) (codified at 50 U.S.C. §1801–11 (1996).

[7] 18 U.S.C. §2518 (3) (1996).

[8] 18 U.S.C. §2511 (1996).

[9] 18 U.S.C. §2516 (2) (1996).

[10] 18 U.S.C. §2518 (3)(c) (1996).

[11] 18 U.S.C. §2518 (5) (1996).

[12] 18 U.S.C. §2518 (8)(d) (1996).

[13] 18 U.S.C. §2518 (9), (10) (1996).

[14] S. Rep. No. 90–1097, at 66 (1968).

[15] Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§2510–21, 2701–10, 3121–26.

[16] See generally S. Rep No 99–541, at 5 (1986); and, H.R. Rep. No. 99–647, at 19 (1986).

[17] 18 U.S.C. §3121–27 (1996).

[18] 18 U.S.C. 2703 (c).

fax and email while in transit. However, ECPA did not extend all of Title III's protections to electronic communications. Unlike Title III, which limits the use of wiretaps to a limited list of crimes, court orders authorizing interceptions of electronic communications can be based upon the violation of any federal felony. While constitutional challenges to the introduction of information obtained in violation of ECPA may succeed, ECPA contains no statutory exclusionary rule as Title III does.[19]

Moreover, Congress et very different rules for access to electronic communications while they are in storage incident to transmission.[20] When the government goes to AOL or another service provider and asks it to provide a copy of a person's email messages from the AOL server where they sit waiting to be read, an ordinary search warrant is enough without the special protections of minimization, judicial supervision and notice to the individual found in Title III.

B. Assumptions of the existing framework

In drafting ECPA Congress began the process of dealing with fundamental changes in technology. They recognized that transactional data needed privacy protections. However, the framework of Title III and the advances of ECPA did not envision the World Wide Web and the pervasive role technology would come to play in our daily lives. Underlying Title III and ECPA were a number of assumptions about both the nature and the use of electronic communications:

- The transmission of private communications and records stored with third parties, including records of such communications, raise different privacy considerations.
- The majority of electronic communications are by nature ephemeral.
- The private sphere of personal communications and interactions would be located at the end-points, not in the medium itself.
- The government's collection and use of information about individuals' activities and communications is the greatest threat to individual privacy.
- Transactional data is not rich in intimate, personal detail.

Congress has only begun to wrestle with the fact that some of these assumptions, while perhaps accurate at one point in history, have changed dramatically since the initial framework for protecting electronic communications was articulated in 1986.

Congress took a first small step towards recognizing the changing nature of transactional data in the networked environment with amendments to ECPA enacted as part of the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[21] The 1994 Amendments recognized that transactional data was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. For example, addressing information was no longer just a number and name, but contained the subject under discussion and information about the individual's location. Therefore, Congress raised the legal bar for government access to transactional data by eliminating subpoena access and requiring a court order, albeit one issued on a lower relevance standard.[22] Some issues were left unanswered, and new ones continue to arise as communications technology advance.

IV. Four examples reveal the current weaknesses of existing statutory protections for privacy in light of the shifts in electronic communications technology and its use in society.

A. Personal papers in cyberspace

Individual's traditionally kept their diaries under their mattress, in the bottom drawer of their dresser or at their writing table. Situated within the four walls of the home these private papers are protected by the Fourth Amendment. With the advent of home computers individual diaries moved to the desktop and the hard-drive. Writers, poets, and average citizens quickly took advantage of computers to manage and transcribe their important records and thoughts. Similarly, pictures moved from the photo album to the CD–ROM.

Today, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. The information has re-

[19] See 18 U.S.C. §2515 (1966) (exclusionary rule refers to wire or oral communications, not electronic communications).

[20] 18 U.S.C. 2703.

[21] Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 and scattered sections of 18 U.S.C. and 47 U.S.C.)

[22] 18 U.S.C. §2703 (b) (A)–(B), (c) (1)(B), (d).

mained the same. A diary is a diary is a diary. But storing those personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed or on the hard-drive. Rather than the Fourth Amendment protections—including a warrant based on probable cause, judicial oversight, and notice—the individual's recorded thoughts may be obtained from the service provider through a mere court order with no notice to the individual at all.

B. Medical records in cyberspace

To bring home what this means in a business setting lets look at medical records. Hospitals, their affiliated clinics and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctors and clinic offices and others. The U.S. government is contemplating the development of a federal governmentwide computer-based patient record system.[23] According to news reports, the Internet and World Wide Web-based interfaces are under consideration.[24] The private sector is moving to integrate network computing into the a sensitive area of our lives—the doctors office.[25]

As computing comes to medicine, the detailed records of individuals' health continue to move not just out of our homes, but out of our doctors offices. While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, and greatly ease billing, prescription refills, and insurance pre-authorizations, it raises privacy concerns.

In the absence of comprehensive federal legislation to protect patient privacy, the protections afforded by ECPA and other statutes are of utmost importance. Unfortunately, the protections afforded to patient data may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual doctor then access to that data will be governed by the Fourth Amendment.[26] Law enforcement would be required to serve the doctor with a warrant or subpoena and the doctor would receive notice and have the chance to halt an inappropriate search. Under federal law, the patient however, would receive no notice and have no opportunity to contest the production of the records. When information is in transit between a doctor and a hospital through a network, law enforcement's access is governed by the warrant requirements of ECPA, and neither doctor nor patient receive prior or contemporaneous notice. If the records are stored on a server leased from a service provider the protections are unclear. They may be accessible by mere subpoena. If they are covered by the "remote computing" provisions of ECPA this would severely undermine privacy in the digital age.[27]

In addition to concerns about government access to personal health information, recent news stories have focused the public on the misuse of personal health information by the private sector—particularly when its digitized, stored and manipulated. Recently the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company. The company was using the information to track customers who failed to refill prescriptions—sending them notices encouraging them to refill and to consider other treatments. Due to public outrage—and perhaps the concern expressed by Senators crafting legislation on the issue of health privacy—CVS and Giant agreed to halt the marketing disclosures.[28] But the sale and disclosure of personal health information is big business. In a recent advertisement Patient Direct Metromail advertised that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections.[29]

---

[23] "Why the Government Wants a Computerized Patient Record," Health Data Network News, Vol. 7, No. 6, March 20, 1998, p.1. "The development of a federal

[24] Id. at 8.

[25] *See generally*, "Six Boston Hospitals Turn To the Internet as a clinicsl Network Tool," Health Data Network News, Vol. 6, No. 6, June 20, 1997, p. 1; "More Clearinghouses Conclude the Internet Makes Economic Sense," Id.; and, "Hospital Banks on Web Technology for Integration," Health Data Network News, Nol. 6, No. 16, Nov. 20, 1997, p. 3.

[26] The record-keeper would have Fourth Amendment protections. Whether the pstient's privacy is protected at all would largely depend upon state law, which is scattered and inconsistent. Until a federal law protecting individusl's privacy in heslth informstion is crafted to protect data regardless of where it is stored or whose control it is under privacy is in danger.

[27] 18 U.S.C. §2703 (b)

[28] "Prescription Fear, Privacy Sales," Washington Post, February 15, 1998, p. A1.

[29] "Medical Privacy is Eroding, Physicians and Patients Declare," San Diego Union-Tribune, February 21, 1998, B1.

The sale and disclosure of what many perceive as less sensitive information is also raising privacy concerns.[30] This past summer AOL announced plans to disclose its subscribers telephone numbers to business partners for telemarketing.[31] AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information.[32] In response, AOL decided not to follow through with its proposal.[33]

As we move forward we must ask, will personal records be afforded differing levels of privacy protection merely because of where and how they are stored? Will individuals be the arbiters of their own privacy, able to make decisions about who knows what about them? How will individual privacy be protected in interactions in the private sector.

C. The case of Timothy R. McVeigh[34]

In January news stories broke about a highly decorated seventeen-year veteran of the U.S. Navy who was to be discharged based on information obtained by the Navy from America Online.[35] The facts surrounding the incident raise many concerns with privacy in the online world. Using an AOL screenname "boysrch," Timothy McVeigh sent an email to a civilian Navy volunteer. The curious volunteer looked up the screenname in AOL's member profile directory and discovered that the subscriber identified himself as "Tim, from Honolulu, Hawaii, employed by the military, and gay." The volunteer passed the screen name and profile information on to her husband, a Navy officer. It eventually landed in the hands of the Judge Advocate General who undertook an investigation. A Navy paralegal called AOL's customer service and asked for information about the subscriber belonging to the screenname "boysrch." AOL identified Timothy R. McVeigh as the subscriber.

According to the administrative separation proceedings, the Navy paralegal had not obtained a warrant, a court order, a subpoena, or Timothy McVeigh's consent prior to contacting AOL, and was therefore in violation of ECPA. In its statement arguing against Timothy McVeigh's request for an injunction, the Navy stated that ECPA puts the obligation on AOL to withhold information, not on the government to follow appropriate procedures.[36] Equally troubling is the fact that because the statute penalizes only "knowing or intentional" violations, it is unclear whether a cause of action will succeed for this violation of privacy and ECPA.

This case illustrates a number of weaknesses of ECPA. ECPA limits the disclosure of information to the government but allows online service providers and others to disclose information, other than the contents of communications, about subscribers to other parties.[37] Is the disclosure of information to the Navy, or more generally the government, an individual's only privacy concern? We can certainly imagine scenarios in which information tying a screenname, and possibly online activities, to an individual's real world identity would substantially invade an individual's privacy and potentially enable further harm to befall him. Of specific concern would be the disclosure of information about children in such a setting. While the government's access to this information, and subsequent actions based upon it, are the source of harm in the McVeigh incident, it is quite possible to imagine a situation equally troubling involving the disclosure of such information to a private party.[38]

---

[30] "Internet power feeds public fear," USA Today, August 13, 1997, A1.

[31] "AOL will share users' numbers for telemarketing," Washington Post, July 24, 1998, E1; "Soon AOL users will get junk calls, not just busy signals and email ads," July 24, 1998, B6.

[32] See letter to Steve Case, President of AOL from the Center for Democracy and Technology, Electronic Frontier Foundation, EFF-Austin, National Consumers League, Privacy Rights Clearinghouse, and Voters Telecommunications Watch.

[33] "AOL cancels plan for telemarketing: Disclosure of member's numbers protested," July 25, 1997, G1.

[34] On January 26, 1998 The United States District Court for the District of Columbia issued a preliminary injunction barring the Navy from dismissing McVeigh.

[35] "Don't chat, don't tell? Navy case tests privacy limits," Wall Street Journal, January 14, 1998, B1.

[36] "AOL says it shouldn't have identified sailor," Wall Street Journal, January 22, 1998, B10.

[37] 18 U.S.C. § 2703 (c)

[38] Privacy concerns with the disclosure of personal information about a specific individual to private citizens and institutions were the impetus behind two recent tightenings of privacy protections. In 1994 the Driver's Privacy Protection Act (DPPA) was passed in response to the murder of Rebecca Schafer, whose killer used department of motor vehicle records to locate her. The law sets limits on the disclosure of motor vehicle operator permits, motor vehicle titles, and motor vehicle registrations by motor vehicle departments. Under the DPPA, individuals must be informed of and given the opportunity to prohibit a) requests for their individual record (an "individual look-up"); and, b) disclosures for the bulk distribution of surveys, marketing or solici-

Continued

A second troubling aspect of ECPA revealed by the McVeigh case is that the lack of a statutory exclusionary rule coupled with penalties that only focus on intentional violations do not create incentives for parties to effectively implement its requirements. In the McVeigh case ECPA itself may not limit the use of the illegally obtained information. While the Constitution may, the lack of a statutory exclusionary rule undermines the goal of assuring that the government follow appropriate procedures designed to protect privacy at the front-end. Similarly, the existing penalty structure set out in ECPA does not encourage proactive behavior to protect privacy. In the incident involving McVeigh, AOL claimed that they did not know they were providing information to a government agent, and therefore under the existing statutory penalties they may not be liable.

D. We know where you are and what you're doing.

An example of the power of transactional data comes from the "location" information available through many cellular networks. In the course of processing calls, many wireless communications systems collect information about the cell site (location) of the person making or receiving a call. Location information can be useful, as Ted Rappaport, the inventor of the hand-held cell phone locator, stated, "If you could know accurately where things are, not only would you feel safer because emergency services could find you, but law enforcement could use it more easily to track the bad guys."[39] But as one reporter put it, "Cellular telephones, long associated with untethered freedom, are becoming silent leashes . . ."[40] The technology is proceeding in the direction of providing more precise location information, a trend that has been boosted by the rulings of the Federal Communications Commission in its "E911" (enhanced 911) proceeding, which requires service providers to develop a locator capability for medical emergency and rescue purposes.[41] Location information may be captured when the phone is merely on, even if it is not handling a call.[42] Private sector uses of this information are also under consideration. A company in Japan is experimenting with a World Wide Web site that allows anyone to locate a phone and the person carrying it by merely typing in the phone number.[43]

In the online environment, transactional data can do more than just track the individual's location. It can provide insight into their thoughts, their affiliations, and their politics. It can reveal whether they are at home or at work. In a world where transactional data captures the full contours of a person's life it is time to provide it with stronger privacy protections.

V. Recommendations

As we consider privacy in the changing communications environment we must ask whether the assumptions of a previous time and technology, and legal distinctions based upon them, continue to make logical sense. Or more importantly, whether they provide protections reflective of our commitment to individual privacy autonomy, dignity, and freedom. Policies designed to implement the Fourth Amendment developed in a 20th century world of paper records—even as extended to protect transient voice communications—may not be applicable to 21st century technologies where many of our most important records are not "papers" in our "houses" but

---

tations. More recently the Individual References Services Group, a group of companies that provide composite profiles of individuals based on data from both public and private sources, crafted a set of self-regulatory guidelines that limit access to their "look-up services." One service offered by IRSG member companies is the ability to access profiles of specific individuals. Like the "indivdualized look-ups" possible at motor vehicle departments or through the IRSG member companies, the disclosure of information to private parties that links an individual to her online identity (screenname) raises privacy concerns. If such information is provided to the wrong person, at the wrong time, it may lead to additional harm to the individual.

[39] "Using cell phones to reach out and find someone: evolving technology will soon be able to pinpoint all mobile dialers," USA Today, December 16, 1997, 6D.

[40] "Technology that tracks cell phones draw fire," New York Times, February 23, 1998, p. D3.

[41] In June 1996, the FCC adopted a Report and Order and Notice of Proposed Rulemaking in Docket 94–102, requiring wireless service providers to modify their systems within 18 months to enable them to relay to public safety authorities the cell site location of 911 callers. Further, the FCC ordered carriers to take steps over the next 5 years to deploy the capability to provide latitude and longitude information of wireless telephone callers within 125 meters. Finally, the FCC proposed requiring at the end of the 5 year period that covered carriers have the capability to locate a caller within a 40 foot radius for longitude, latitude and altitude, thereby, for example, locating the caller within a tall building. In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., CC Docket No. 94–102, Report and Order and Further Notice of Proposed Rulemaking (last modified Jan. 2, 1997) [hereinafter FCC E–911 Order]
<http://www.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt>.

[42] Albert Gidari, *Locating Criminals by the Book*, CELLULAR BUS. (June 1996) at 70.

[43] "The scariest phone system," Fortune, October 13, 1997, p. 168.

"bytes" stored electronically and our communications rather than disappearing into thin air are captured and stored at distant "virtual" locations for indefinite periods of time.

To address privacy in the electronic communications environment the Congress should:

Reexamine the need for limits on the disclosure and use of personal information by private entities. Both the Federal Trade Commission and the Department of Commerce are engaged in initiatives designed to promote "fair information practice principles" in the online environment. We are encouraged that Congress is exploring protections for individual privacy during private sector activities. In considering this issue we recommend that discussions focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare (HEW) in 1973[44] and the Guidelines for the Protection of Privacy and Transborder flows of Personal Data, adopted by the Council of the Organization for Economic Cooperation and Development in 1980.[45]

Reconsider how the lines have been drawn between records entitled to full Fourth Amendment protection and business records[46] that fall outside the protection of the Fourth Amendment. There are now essentially four legal regimes for access to electronic data: (i) the traditional Fourth Amendment standard, for records stored on an individual's hard drive or floppy disks; (ii) the Title III–ECPA standard, for records in transmission; (iii) the business records held by third-parties, available on

---

[44] 1.There must be no personal data record-keeping systems whose very existence is secret;

2. There must be a way for an individual to find out what information is in his or her file and how the information is being used;

3. There must be a way for an individual to correct information in his or her records;

4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and

5.There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U.S. Dept. of Health, Education & Welfare, July 1973.

[45] 1. Collection limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data a re collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

— within a reasonable time;

— at a charge, if any, that is not excessive;

— in a reasonable manner; and,

— in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[46] In 1976 with *US* v. *Miller*, the Supreme Court began a line of cases holding that individuals have no constitutionally protected privacy interests in personal information contained in the business records held by third parties. In 1979, in *Smith* v. *Maryland*, the Court applied *Miller* to the electronic world ruling that the use of a pen register to collect the phone numbers dialed on a surveilled line did not implicate Fourth Amendment interests. While Congress responded to both decisions crafting procedural rules to govern law enforcement access to bank and telephone records, the Miller and Smith decisions leave personal information divulged or generated during business transactions without privacy protections—unless Congress steps in to craft them. *United States* v. *Miller*, 425 U.S. 435 (1976); *Smith* v. *Maryland*, 442 U.S. 735 (1979).

a mere subpoena with no notice to the individual subject of the record; and, (iv) a third, the scope of which is probably unclear, for records stored on a remote server, such as the research paper (or the diary) of a student stored on a university server or the records (including the personal correspondence) of an employee stored on the server of the employer. As the third and fourth categories of records expand because people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Heighten the standard for access to transactional data. Transactional data are in many ways a person's digital fingerprints, although far more easily captured. Transactional records provide unprecedented information about the places, people, and activities that comprise the individual's daily life.

Create a privacy entity to provide expertise and institutional memory, a forum for research and exploration, and a source for guidance and policy recommendations on privacy issues. The existing crisis-driven approach to responding to privacy concerns has hindered the development of sound rational policy and failed to keep pace with changes in technology. The US needs an independent voice empowered with the scope, expertise, and authority to guide public policy. Such an entity has important roles to play on both the domestic and international fronts. Without an independent voice, privacy rights in the United States will not be afforded adequate consideration and protection in emerging media.

Encourage the development and implementation of technologies that support privacy on global information networks. Technological mechanisms for protecting privacy are critically important on the Internet and other global medium. Developing meaningful privacy protections in the online environment requires us to realize that our laws and Constitutional protections may not follow our citizens, their communications, or their data as it travels through distant lands. Technology can provide protections regardless of the legal environment.

Strong encryption is the backbone of technological protections for privacy. Today technical tools are available to send anonymous email, browse the World Wide Web anonymously, and purchase goods with the anonymity of cash. The World Wide Web Consortium's Platform for Privacy Preferences, currently under development, will provide an underlying framework for privacy—allowing Web sites to make their information practices available to visitors and individuals to set privacy rules that control the flow of data during interactions with Web sites.[47] This effort has involved non-profit, for-profit and government representatives.

The U.S. should encourage the development of privacy-enhancing technologies that address the need either to eliminate data collection, or where data collection occurs: to limit the data collected; to communicate data practices; and, to facilitate individualized decision-making where consistent with policy.[48]

Collaborate with other governments, the public interest community and the business community to develop global solutions for the decentralized network communications environment.

Traditional top down methods of implementing policy and controlling behavior, be they international agreements, national legislation, or sectoral codes of conduct enforced by the private sector, offer incomplete responses to the privacy issues arising on the global information infrastructure. Implementing privacy policy in the decentralized, global and borderless environs of international networks raises difficult questions of effectiveness and enforcement. The U.S. should work with all parties—other governments, international bodies, the public interest and for-profit communities to build consensus on appropriate policy. Providing a seamless web of privacy protection to individuals' data and communications as it flows along this international network may require new tools—legal, policy, technical and self-regulatory—for implementing policy. The U.S. should actively participate in their crafting.

Thank you for the opportunity to participate in this important discussion about protecting privacy in the online environment.

Mr. COBLE. Mr. Rotenberg.

---

[47] Public drafts of the specification and implementation guide should be available shortly at http://www.w3c.org/

[48] These incorporate the basic concepts of three recommendations of the Danish and Canadian Privacy Commissioners:

> eliminate the collection of identity information, or if it is needed keep it separate from other information; minimize the collection and retention of identifiable personal information; and, make data collection and use transparent to data subjects and provide them with the ability to control the disclosure of their personal information, particularly identity information.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman, and thank you for the opportunity to be here this morning. I would also like to thank the subcommittee for your work in support of Representative Goodlatte's legislation, the Safe Bill, which for many users on the Internet is very important to us.

These issues of privacy on the Internet at times appear very complicated, new software, new techniques, browsers, Cookies, and it seems as if there are no clear lines. Why should the government regulate if the technology is changing so quickly or if the expectations are so unclear.

But in fact privacy policy and privacy law is based on a simple set of principles. It is that when you give up personal information you gain certain rights, and when organizations acquire your information they take on certain responsibilities. This is true with your bank, with your telephone company, with your doctor and with the Federal Government.

These practices, these policies are generally referred to as "codes of Fair Information Practices," and they can be found in every privacy law in the United States and around the world. They give rights to individuals, and they establish responsibilities for organizations that hold information.

None of this has changed with the Internet. When a company sets up a business on the Internet and acquires your information they have responsibilities, and those responsibilities to be effective need to be backed up, as they have always been, by a right in law to seek redress when a harm occurs.

But what has changed with the Internet in this new era of technology is the opportunity to use technology to protect privacy. You see, much of our law is based on the view that technology is a threat to privacy, that Big Brother will be able to use these big databases to keep track of all our private activities. But we also see that there are now ways with techniques, such as encryption, to protect our communications and to protect our identity. So, the second critical aspect of privacy on the Internet is to make available these techniques so that people can protect their privacy.

Now Ambassador Aaron testified on the earlier panel that encryption was not widely used and was not particularly significant, and I have to disagree with him on this point. In the past week I have purchased a book online at Amazon.com. I entered my credit card number at my keyboard to make that purchase possible and, fortunately, the software that I was using provided by Netscape encrypted that link, that communication between me and the online merchant so that my credit card number would not be disclosed to others.

And yesterday I helped my wife change her user ID with our local service provider. I went in through Internet Explorer. (We are bipartisan with browser software as we are in politics.) And, fortunately, Microsoft has provided encryption so that when I was communicating her user ID across the Internet and the password it would not be available to others. My experience is the same experience as millions of people using the Internet today. They need these new techniques to protect their privacy.

Cutting to the bottom line, the problem is that our current privacy policy, the policy that is reflected today in the position of the White House and the Administration is exactly backward. Where we need to step aside and let these new techniques develop and let free market ingenuity and innovation do what they do well the government is trying to impose controls. They don't want strong encryption, they don't want anonymous payment schemes, they don't want telephone services that can't be wiretapped. That is the wrong approach.

But where government help is needed because privacy rights aren't being enforced, because there isn't redress for consumers, and because we haven't extended fair information practices to new services the government is standing on the sidelines and saying you all figure it out. The problem with this policy can be seen when you compare our current policy with what is taking place in other countries today as well as with our own history.

Let me propose for you, for example, to consider the significance of the date October 1998, just a few months from now. In Europe that is the date where a comprehensive privacy law goes into force. It's not a perfect law. Like most laws it has got some problems, but it does reflect a fundamental commitment to protect the rights of citizens and their privacy.

In the United States in October we're going to put in place the digital telephony bill which requires that all telephone networks be capable of police surveillance. We are promoting surveillance. Other countries are wrestling with the issue of how to protect privacy. This is an urgent issue. We have to change course. Privacy today is the No. 1 concern of Internet users, and without strong safeguards people will not use the Internet.

We think we have a common interest in solving this problem, and I very much appreciate the chance to be here this morning.

Mr. COBLE. Thank you, Mr. Rotenberg.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

SUMMARY

Public opinion polls show that privacy is the number one concern of Internet users. Everyone is aware that a great deal of personal information is collected, and that virtually no meaningful protections are in place.

In the McVeigh-AOL case, a person almost lost his job because of information that was improperly disclosed by an online service provider. An amendment to Electronic Communications Privacy Act could help prevent similar incidents in the future. But the example is just one of the many privacy risks that people using the Internet today face.

The Internet lacks adequate privacy protection. A survey by the Electronic Privacy Information Center in 1997 of the 100 top web sites found that less than half had privacy policies, and those with policies offered little real protection. Still, anonymity plays a critical role in online privacy as it gives individuals the ability to control the disclosure of their identity.

Even though the Internet is a very new communications environment, the commitment to establish privacy protection by law in the United States is long-standing. The US developed important legal safeguards to protect the privacy of communications and established the fundamental approach to the protection of personal information—generally described as "Fair Information Practices"—that make clear the responsibilities of organizations that collect data and the rights of individuals who give up personal information.

But our policies US have not kept up to date. The absence of new legal protections for privacy coupled with government efforts to restrict the use of new privacy enhancing techniques, such as encryption, have produced a privacy policy that is almost exactly backward. This becomes particularly clear if you contrast our current policy with our own history of privacy protection and current developments in other parts of the world.

Several steps must be taken to set our privacy policy back on course. First, enforceable Fair Information Practices should be applied to the Internet. This is best done by legislation. The self-regulatory approach is not working. Second, techniques to protect privacy and anonymity should be encouraged and restrictions on encryption should be lifted. Finally, a privacy agency should be established to develop additional recommendations for privacy protection and to provide permanent leadership within the federal government on this important issue.

We are at the beginning of a long and difficult period for the protection of privacy in this country. Technology is racing ahead. Our laws and institutions are lagging far behind. The level of public concern about privacy is growing. There is much work to be done.

My name is Marc Rotenberg. I am the Director of the Electronic Privacy Information Center, a non-partisan research organization in Washington, DC. I am an adjunct professor at Georgetown University Law Center and Senior Lecturer at the Washington College of Law. I am also editor, with Philip E. Agre, *of Technology and Privacy: The New Landscape* (MIT Press 1997).

I appreciate the opportunity to testify before the Subcommittee today. I'd like to thank the Subcommittee for holding this hearing and also for your ongoing work in support of Representative Goodlatte's SAFE bill that would help reform our nation's policy on encryption.

McVeigh-AOL Case

The growing concern about the loss of privacy on the Intenet was made clear earlier this year when the Navy began discharge proceedings against a decorated sailor based on personal information about the sailor disclosed by America Online. A Navy investigator, suspecting that Mr. McVeigh might be in violation of the "Don't Ask, Don't Tell" policy, obtained information that linked Mr. McVeigh's "screen name," which was not his actual identity, with his real identity. Once the connection was established, the discharge proceeding began.

The McVeigh-AOL case raised a complicated set of legal issues. The AOL Terms of Service agreement specifically prohibited this disclosure.[1] But a civil action against the company would not mean reinstatement by the Navy. The disclosure also appeared to violate the Electronic Communications Privacy Act, but the statute is ambiguous about the remedies available to victims of such disclosure.

Mr. McVeigh filed suit against Navy Secretary John Dalton in federal court. Judge Stanley Sporkin found that the Navy had violated the "Don't Ask, Don't Tell policy" when it pursued the investigation. In the course of the decision, Judge Sporkin also considered whether the Navy violated the Electronic Communications Privacy Act.[2] The opinion is a little less clear on this point. Judge Sporkin said the investigation undertaken by the Navy was "likely illegal" under the ECPA because the Navy investigator failed to obtain a warrant before he sought personal information from America Online about Mr. McVeigh. The government contended that the obligation to comply with ECPA fell not on the government actor but rather on the online service provider.[3]

Judge Sporkin said that the statute read as a whole made clear the intent to regulate the conduct of government agents. He found that even if the relevant provision did not apply to the actions of government (18 USC § 2703), "it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated." Judge Sporkin concluded "in these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks

---

[1] America Online, Terms of Service Agreement and Rules of the Road:

"Our policy is not to disclose identity information to third parties that would link a Members screen name (s) with a Members actual name, unless required to do so by law or by legal process served on AOL, Inc. (e.g., a subpoena). AOL, Inc., at its sole discretion, reserves the right to make exceptions to this policy in extradordinary circumstances (such as a bomb or suicide threat, or instances of suspected illegal activity) on a case-by-case basis."

5(B)(iii) Privacy Policy—Member Identity and Billing Information.

[2] 18 U.S.C. §§ 2501, et. seq. (West 1997).

[3] Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996) (Section 2703(c)(1)(B) only prohibits the actions of online providers, not the government).

of life are being ignored or marginalized, it is imperative that statues explicitly protecting these rights be strictly observed."

The McVeigh case is critical for several reasons. First, it makes clear that privacy violations have real consequences. Mr. McVeigh's life was forever changed by the decision of America Online to disclose personal information about him to his employer. Second, the case shows the shortcomings of contractual solutions. Even with a very clear contract provision detailing when personal information may be disclosed, the Navy investigator was still able to obtain personal information about Mr. McVeigh. Third, the case shows that we are all becoming increasingly dependent on these new services to safeguard our privacy. America Online today has more than eleven million subscribers.

Mr. McVeigh's case, because the improper disclosure of information was so well documented, received national attention. But there are many other people in this country who face similar privacy risks, whose names will never be known. Indeed, they themselves may never know that information about them was improperly disclosed.

What is Privacy?

In some respects, the McVeigh case appears complicated. AOL didn't actually disclose personal information about Mr. McVeigh, such as an unlisted phone number or a Social Security Number. Rather, the company disclosed information that linked his actual identity to an assumed identity. The Internet raises many privacy issues that seem novel or unusual:

- Search engines allow people to find information all across the Internet but can also store the identity of the user and the inquiry the person made. Should this information be saved, should it be disclosed or sold, or used for marketing?
- Copyright management systems will record the individual use of digital works such as books sold online and newspapers read over the Internet. Should personally identifiable information be collected or should techniques to protect anonymity be pursued?
- Internet software makes it possible to track the web sites that a user visits and the pages he or she views. Should advertisers compile individual preferences to customize ads or place products on web displays?
- Operators of web sites can easily collect a great deal of information from individuals, far more than would be available in a typical commercial transaction. Should companies collect this information, use it, or it?
- Marketers are developing one-to-one marketing techniques specifically designed to target young people. Are special privacy safeguards necessary for children?
- Internet Service Providers provide a critical gateway to the on-line world. Should they have a special obligation to protect privacy and be subject to legal rules?

As complicated as these examples may seem, the basic privacy analysis is not so difficult. The premise that virtually all privacy law and policy is based on is the belief that when individuals give up personally identifiable information to organizations, the organizations take on some obligation and the individuals are granted some rights. We call these responsibilities and rights "Fair Information Practices."

The critical elements of Fair Information Practices include:

- Distinguishing personally information from other information. Demographic data and aggregate data generally do not raise privacy concerns, but data that can be a linked to a specific, identifiable individual does raise a privacy issue.
- Articulating the responsibilities of data collectors, such as the responsibility to limit disclosure of personal information, to ensure that it is used for the purpose collected, and to provide adequate security to protect that data
- Articulating the rights of data subjects, such as the right to inspect and correct data, to seek redress, and to receive damages

You will find this approach to privacy protection in virtually all of the privacy laws in the United States, including many of the recent statutes that address new technologies, such as the subscriber privacy provision in the Cable Act of 1984, the Electronic Communications Privacy Act of 1986, the Video Privacy Protection Act of 1998 (video tape rentals), the Telephone Consumer Protection Act of 1991 (auto-dial-

ers and junk faxes), and even the CPNI rules contained in the Telecommunication Reform Act of 1996 (customer billing information).

To be effective, Fair Information Practices must be enforced and must provide redress. It is not enough to say what a policy is without providing a means to enforce the policy. That is why voluntary guidelines, professional standards, and codes of conduct that are based on Fair Information Practices do not necessarily provide significant privacy protection.

There are also some novel issues.[4] One very interesting and very important policy question is brought about by the development of new technologies that make it possible to protect privacy in ways we had not previously imagined. Traditionally, we understood that technology was a threat to privacy and that it was the proper role of government to restrict the use of techniques that might intrude on privacy. But now we see in such techniques as public key encryption and anonymous payment schemes the opportunity to develop new means to limit the disclosure of personal information.

The critical question then becomes what role government should play in promoting, regulating, or restricting techniques such as encryption that allow individuals to protect personal information. In the United States this debate has largely been framed in terms of the need to balance the interests of privacy and commerce against the concerns of law enforcement and national security. But in most other parts of the world that have looked at this issue, there is a very different view. Many governments believe that these new technologies should be promoted and that efforts to impose controls for law enforcement purposes are short-sited and will ultimately prove futile.[5]

In my view, privacy in the information age means both the extension of Fair Information Practices to new information environments and the active promotion of techniques, often based on encryption, to protect the disclosure of personal information. This is the fundamental policy goal.

Understanding the Problem of Privacy on the Internet

To understand the problem of privacy on the Internet in more detail, EPIC conducted a survey of the top 100 web sites in the summer of 1997.[6] It was the first comprehensive survey of Internet privacy. We looked at the policies and practices actually in place on the most popular web sites. For each site, we checked whether personally identifiable information was collected, whether a notice describing privacy polices was displayed, whether the policy was adequate, and similar questions.

We found that about half of the sites that we surveyed collected personal information. This was typically done for on-line registration, surveys, user profiles and order fulfillment. Seventeen sites had privacy notices or statements, but the policies were often not easy to locate and some policies we could only find after we registered at the site.

We believed it was important to look not simply at whether the site had a privacy policy. It is critical that a privacy policy explain the responsibilities of organizations collecting data and rights of the person who provides data. We found that few of the sites provided adequate protection. A critical question for the future of Internet privacy will be whether there is a means to enforce Fair Information Practices.

One of the most interesting findings in our survey was that anonymity was largely respected by the websites. Most websites allow users to visit and receive information
about products, or news, or almost anything else you can find on the Internet without collecting personal information.

In the conclusions of our report we said that:

- Webs sites should establish a privacy policy that is easy to find
- Policies should state clearly what personal information is collected and how it will be used
- Web sites should make it possible for individuals to access their own data
- Cookies transactions should be more transparent
- Anonymity should be encouraged

---

[4] P. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press 1997).

[5] Organization for Economic Cooperation and Development, *Cryptography Policy Guidelines* (1997) [http://www.oecd.org/dsti/iccp/crypto—e.html].

[6] Electronic Privacy Information Center, "Surfer Beware: Personal Privacy and the Internet," (June 1997) [http://www.epic.org/reports/surfer-beware.html].

We closed with the warning "surfer beware" because we concluded that there was simply too little privacy protection on the Internet for users to feel secure, and we hoped stronger privacy standards would be developed.

Several web operators wrote to us after Surfer Beware was released to say that they were developing privacy policies for their sites.[7] The New York Times web site added a privacy policy a few days after our report came out. The response has been very good.

This month the Federal Trade Commission is conducting a similar survey of 1,200 web sites.[8] I suspect that the FTC will find that a growing numbers of web sites do now have privacy polices. But whether those policies are meaningful or provide any redress to users of these services remains unclear. It is worth noting that America Online has one of the most comprehensive and detailed privacy policies of any company operating on the Internet today. And still Timothy McVeigh almost lost his job.

History of Communications Privacy

One of the great achievements of the American legal system has been our strong commitment to protecting the privacy of personal communications. You can trace this history back at least as far as Benjamin Franklin, who in establishing the national postal service recognized the need to enact federal law to protect the privacy of communications.[9]

But it was not until 1928 that the Supreme Court had its first brush with the question of whether our Bill of Rights, drafted in the eighteenth century, would apply to the new communications technologies of the twentieth century and beyond. The case concerned a highly successful bootlegging operation in the Pacific Northwest operated by Ralph Olmstead. Federal agents began an extensive surveillance operation that lasted for more than five months. They had no recording devices, so they wrote down what they heard. Sometimes they relayed their recollections of conversations to a stenographer. In the end, they compiled more than 775 pages that they brought to court. The issue was whether the Fourth Amendment warrant requirement would be applied to this new investigative technique. The trial court let the evidence in, over the objection of Mr. Olmstead, and the appeals court affirmed.[10]

When the case finally reached the Supreme Court Chief Justice William Taft wrote a detailed opinion that focused on the absence of a physical search, of the type proscribed by the Fourth Amendment, and concluded that the evidence was admissible. The Court held that the Fourth Amendment simply did not apply to this new form of communication.[11]

But there were two important dissents. Justice Holmes called the matter a "dirty business" because the federal agents had violated a Washington state law that prohibited wiretapping to obtain the evidence. He voted to reverse.[12]

Justice Brandeis also dissented.[13] His opinion was not so much about the illegal acts of federal agents; he was more interested in the question of how the Fourth Amendment and our Constitution generally, should apply to these new communication technologies. He wrote, in one of the most famous phrases in American law, that the makers of our Constitution "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of all rights and the right most valued by civilized men."[14] Brandeis's dissent in *Olmstead* reminds us that the protection of privacy is at the heart of our system of ordered liberty and that that law is an evolving process.

The Supreme Court eventually adopted Justice Brandeis's view and decided in 1967 that the Fourth Amendment did indeed apply to telephone communications.[15] Following the Katz decision and a related case, Berger v. New York,[16] the Congress

---

[7] See, e.g., note from Steve Jenckins, webmaster, Windows95.com ("We had previously been unaware of these privacy concerns, and thank you for bringing them to the attention of surfers across the 'Net, and to Webmasters of major sites.")

[8] Federal Trade Commission News Release, "FTC Staff To Survey Consumer Privacy on the Internet" (Feb. 26, 1998) [http://www.ftc.gov/opa/9802/webcom2.htm].

[9] David Seipp, "The Right to Privacy in American History," Program in Information Resources Policy, Harvard University (1977)

[10] Alan Barth, Prophets with Honors: Great Dissents and Great Dissenters in the Supreme Court 54–79 (1975)

[11] 277 U.S. 438, 455 (1928).

[12] Id. at 469.

[13] Id. at 471.

[14] Id. at 473.

[15] U.S. v. Katz, 389 U.S. 347 (1967).

[16] 388 U.S. 41 (1967).

set out in 1968 to establish a framework to allow electronic wiretapping only under the most limited circumstances. The Congress made clear at that time that wiretapping was to be an investigative means of "last resort."

While some have said that Title III makes clear that the police have the right to wiretap telephone communications when a court order is obtained, I believe the better view of the Act is that it ensured that electronic surveillance would be brought within strict Fourth Amendment requirements. In other words, our federal wiretapping statute was intended to limit this investigative technique to the narrowest circumstances.

Since 1967 there have been a number of significant developments in the law of communications privacy. In 1978 the Congress passed the Foreign Intelligence Surveillance Act to deal with the difficult problem of wiretapping of foreign agents. The Supreme Court had left open the question in the Katz case of whether the Fourth Amendment should apply to national security cases. The Congress resolved this question with the FISA in 1978, establishing a Title III-like framework, albeit with more secrecy and less accountability.[17]

In the mid-1980s the growth of the Internet and new communications services was apparent. People were using desktop computers and sending messages to one another by means of electronic mail. Questions about the appropriate standards for government searches were arising. In response, Congress amended Title III and enacted the Electronic Communications Privacy Act, which extended privacy protection to stored electronic communications.

The next significant development came in 1994 when Congress passed the Communications Assistance for Law Enforcement Act (CALEA), a measure commonly referred to as "digital telephony." CALEA gave the Department of Justice the authority to set technical standards for the nation's telephone system in an attempt to ensure the ongoing viability of wiretapping.

Many said at the time that the measure was considered that it was a mistake to pass such legislation, not only because it was a fundamental change in the law's approach to electronic surveillance and police powers generally, but also that the bill would be impractical and ultimately unworkable.

For better or worse, this predication seems now to be correct. The FBI and the telephone industry are mired in endless debates about implementing the legislation, the estimated costs are far beyond the initial authorization, the technology innovations continue, and the CALEA policy has slowed the adoption of technical methods, such as encryption, that could make our communications network more secure and reduce the risk of crime. Moreover, our government is now in the unfortunate position of urging other nations to develop more extensive surveillance capabilities.

I hope at some point in the future the Judiciary Committee will have the opportunity to revisit CALEA and to consider whether this is still a sensible policy initiative.

The Role of Government

The United States was for many years a leader in efforts to protect personal privacy. Justice Brandeis wrote a famous law review article on the right to privacy in the late nineteenth century that established the legal claim in this country and elsewhere.[18] The privacy right came to be described as the "American tort."

Many other countries joined the US effort to firmly establish this right following the end of the Second World War. The Universal Declaration of Human Rights was adopted and the right of privacy was made explicit in the constitutions of many governments.

The United States continued to lead in the modern era of privacy protection with passage of the Fair Credit Reporting Act in 1970 and then with the Privacy Act of the 1974 that provided comprehensive privacy protection for records held by the federal government.

But our lead has slipped, and we are now viewed by many as falling behind in the effort to protect this critical right. The Administration's own record on privacy protection has been very poor. Not only has the White House resisted calls from long-time trading partners and allies to develop stronger privacy measures, it has actively opposed efforts by other governments to extend privacy rights to their own citizens. This combined with the Administration's attempt to extend techniques for electronic surveillance has placed the United States in the unfortunate position of promoting state surveillance as other governments are trying to establish privacy protection.

---

[17] 50 U.S.C. §§ 1801–1811.

[18] Warren & Brandeis, "The Right to Privacy," 4 Harv.L.Rev. 1 (1890).

The sharp contrast in our government's approach to privacy issues, when compared with other governments, can be understood by considering the significance of the date "October 1998." In Europe that is the date when the European Data Directive goes into force. It is a comprehensive privacy measure that establishes rights for citizens and recognizes that privacy protection will remain critical for the information economy. It is the result of many years of hard work, negotiation, and commitment by lawmakers.

In this country, in October 1998, we will mark the date when the Communications Assistance for Law Enforcement Act is expected to be operational. That is the law, as I have noted, that requires telephone companies to try to protect electronic interception in the nation's telephone system. We are pursuing elaborate and expensive policies for national communications surveillance as other countries are struggling with the issue of how to protect the privacy rights of their citizens.

We are today not only behind the curve in developing sensible privacy polices, but we are largely out of step with the rest of the world. Lacking the formal means to develop privacy policies and to respond to public concerns, we have left the law enforcement community and the marketing industry to determine how much privacy there will be in the future. The result is not surprising—there is growing public concern about the loss of privacy and a widening gap between the problems we face and the solutions we should pursue.

Simply stated, our policy is backward. We impose government controls on techniques to protect privacy, where market-based solutions are preferable. And we leave privacy problems to the market, where government involvement is required.

Recommendation

Today the calls for government action to protect privacy are unambiguous. The most recent Harris poll found that a majority of those polled found that privacy is the main reason that people are staying off of the Internet. They want legislation now to protect privacy on the Internet.[19] According to the BusinessWeek/Harris poll, 53% believe that "Government should pass laws now for how personal information can be collected and used on the Internet." Of those polled, 23% said "government should recommend privacy standards for the Internet but not pass laws at the time." Only 19% believe that the government "should let groups develop voluntary privacy standards but not take any action now unless real problems arise."

The Harris/BusinessWeek poll is consistent with other polls that have asked similar questions about privacy and the Internet. Contrary to the popular view that Internet users oppose all form of government action, when it comes to matters of privacy, they believe new laws are necessary.[20]

Much is also said about the desirability of "self-regulation" for the Internet. There are, indeed, many areas where the government can do the most by doing the least. This is particularly true with matters of speech and content, where our strong First Amendment tradition cautions against any attempt by government to regulate what people may say, read, or watch. But self-regulation has not helped protect privacy on the Internet. It has in fact made it harder for us to focus on the larger questions of a coherent privacy policy. It has also led to erosion in our basic understanding of privacy protection.

For example, the concept of Fair Information Practices—the common thread of all privacy law and policy that clearly places responsibilities on organizations and gives rights to individuals—is now being revised to suit the needs of organizations rather than to protect the interests of individuals. Where once there was an understanding that individuals should have the right to get access to their own data, to inspect it, and to correct it, now those who favor self-regulation believe it is necessary only to provide access to a privacy policy.

Where once individual *consent* was central to the disclosure of personal information, now the focus is on individual *choice* for a range of disclosures. Where privacy techniques focused on the means to protect identity, now the focus is on means to obtain information. Many of the techniques that are put forward as "technical solutions"—such as the Open Profiling Standard, the P3P and Trustee—will make it easier, not more difficult, to obtain information from individuals using the Internet. Something is clearly amiss.

It is time to reestablish support for Fair Information Practices, to make clear that organizations that collect information have responsibilities, and that individuals

[19] BusinessWeek, "A LITTLE NET PRIVACY, PLEASE: Netizens want immediate action from industry and government as consumer-data gathering exceeds the comfort zone." (Mar. 16, 1998) [http://www.businessweek.com/1998/11/b3569104.htm].

[20] GVU 8th WWW Survey. [http://www.gvu.gatech.edu/user—surveys/survey-1997–10/]

who give up information have rights. The principles are well established in our legal tradition. Privacy protection should not end where the Internet begins.

Amend the Electronic Communications Privacy Act

Congress should specifically consider expanding the scope of privacy provided to subscriber information under Section 2703 of ECPA. Currently, the statute only prohibits the disclosure of such data to "governmental entities" unless they obtain legal process authorizing the disclosure. This prohibition should be extended to the disclosure of subscriber information to *any* third party. One of the reasons why the Navy was able to obtain information concerning Mr. McVeigh from AOL is that ECPA places no restrictions on service providers unless the requester identifies himself as a government agent, which the Navy investigstor failed to do. Further, the current statutory regime fails to recognize that significant harm can result from the disclosure of personal information to non-governmental actors. Had Mr. McVeigh been a private sector employee, ECPA would have provided absolutely no protection, despite the fact that he could have lost his job in much the same way. *Any* requester should be required to provide legal authorization before receiving personal information from a service provider.

With respect to governmental access, ECPA should be amended to prohibit the use as evidence of information obtained in violation of Section 2703, in the same way that Section 2515 prohibits the use of illegally obtained wire or oral communications. Finally, the civil action provision contained in Section 2707 should be amended to make clear that a cause of action will lie against a governmental entity that obtains information in violation of Section 2703.

Support Passage of Internet Privacy Bill and the Children Privacy Bill

The Consumer Internet Privacy Protection Act of 1997 (HR 98) would prevent an "interactive computer service" from disclosing to a third party a subscriber's personal information without that individual's written content. This is a good starting point but will leave uncovered many areas that should receive protection. Representative Franks bill, the Children Privacy Protection and Parental Empowerment Act also provides important safeguards.

Establish a Privacy Agency

In 1973 the Department of Health, Education and Welfare established a special panel to study privacy issues arising from the growing use of automated date processing equipment.[21] That report led to the development and passage of the Privacy Act of 1974, perhaps the most important privacy law in our country. But that report also made clear, as have subsequent reports, that the cornerstone of an effective federal policy is a permanent privacy agency.

It is critical today that a privacy agency be established. We simply do not have the expertise, commitment, or understanding in the federal necessary to develop the policies necessary to address the enormous challenges that we are facing. Many of the decisions that are made with significant consequences for privacy protection lack adequate representation of privacy concerns.

In countries across the world, efforts are underway to address these privacy concerns. The European Union is moving forward on the implementation of extensive privacy directive that will establish legal rights for all citizens in the European Union countries. Non-EU countries, including Japan and Canada, are pursuing comprehensive privacy polices. Techniques for anonymity are being promoted in Germany, the Netherlands and elsewhere. Strong medical privacy legislation is in place in New Zealand.

In the United States, even with the efforts of the Federal Trade Commission, there is little sense that we are making progress. Privacy concerns are rising. The public is not persuaded by the current policy. BusinessWeek put it well in an editorial earlier this month:

> Time is running out for the Net community. The public does not trust its promises for self-regulation to ensure privacy. The polls show that people don't believe that these voluntary standards are working. Any spot check of Web sites shows that few make any serious effort to protect privacy. It's no wonder that the public wants the government to step in immediately and pass laws on how personal information can be collected and used. Even Silicon Valley libertarians who believed in voluntary standards for years are no longer so sure.
>
> As the economy shifts increasingly from an industrial to an information base, an individual's private data take on an economic utility unknown in the past. So, too, does a person's economic behavior in the electronic realm. Future

[21] *Records, Computers, and the Rights of Citizens* (1973).

growth depends on the security of that data and the comfort level for that behavior. Both civil society and economic growth depend increasingly on privacy.[22]

The United States has long been a beacon of individual liberty and a champion of individual rights. Our greatest challenge today is to carry forward that tradition into the information age. For Internet users today and into the future, that will mean protecting the right of privacy.

References

P. Agre and M. Rotenberg, eds., *Technology and Privacy: The New Landscape* (MIT Press 1997)

J. Cohen, "A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace," *U.Conn.L.Rev.* (1996)

W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press 1997)

S. Friewald, "Uncertain Privacy: Communication Attributes After The Digital Telephony," 69 S. Cal. L. Rev. 949 (1996)

International Working Group on Data Protection, Data Protection and Privacy on the Internet, *Data Protection and Privacy on the Internet* (1996) [http://www.datenschutz-berlin.de/diskus/13—15.htm]

National Information Infrastructure Task Force, Information Policy Committee, "Options for Promoting Privacy on the National Information Infrastructure" (1997)

Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) [http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM]

Organization for Economic Cooperation and Development, *Cryptography Policy Guidelines* (1997) [http://www.oecd.org/dsti/iccp/crypto—e.html]

P. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995)

M. Rotenberg, "Communications Privacy: Implications for Network Design," *Communications of the ACM* (1995)

M. Rotenberg, "Data Protection in the United States—A Rising Tide?" *The Computer Law and Security Report* 38–40 (January-February 1998)

M. Rotenberg, "In Support of a Privacy Protection Agency in the United States," *Government Information Quarterly* (Winter 1991)

P. Schwartz and J. Reidenberg, *Data Privacy Law* (Michie 1996)

B. Schneier and D. Banisar, *The Electronic Privacy Papers* (John Wiley 1997)

[22] BusinessWeek, "Privacy: The Key to the New Economy," p. 128 (Mar. 16, 1998).

ELECTRONIC PRIVACY INFORMATION CENTER

SURFER BEWARE:
PERSONAL PRIVACY AND THE INTERNET

June 1997

Electronic Privacy Information Center
Washington, DC
http://www.epic.org/

SUMMARY

The Electronic Privacy Information Center (EPIC) reviewed 100 of the most frequently visited web sites on the Internet. We checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity. We found that few web sites today have explicit privacy policies (only 17 of our sample) and none of the top 100 web sites meet basic standards for privacy protection. However, anonymity continues to play an important role in online privacy, with many sites allowing users to access web services without disclosing personal data. EPIC recommends that sites continue to support anonymity while developing policies and practices to protect information privacy.

INTRODUCTION

The protection of privacy is one of the most important issues on the Internet today. Internet users routinely report that privacy protection is one of their greatest concerns. More Internet sites are collecting personal information from users through online registrations, surveys, and forms. Information is also collected from users surreptitiously with "cookies." Web users are understandably concerned about the potential loss of privacy.

We set out to determine what privacy policies and practices were actually in place on the most popular web sites today. We were interested in determining when personal information was being collected. We wanted to see if web sites had explicit privacy policies and how good those policies were. We were curious if sites made it possible for individuals to view their own information collected at the site. We checked to see if users could visit a site anonymously. We also wanted to look at the use of cookies. A summary of our findings follows. The complete survey is in the Appendix.

SCOPE OF SURVEY

We surveyed the Top 100 web sites as reported by www.100hot.com on June 5, 1997. According to 100hot, the site "lists the most popular sites on the web excluding browser companies, ISP's, colleges, and Adult sites." The list is compiled daily in cooperation with Alta Vista.

We are aware that there are several other services that compile lists of popular Internet sites, but we think the 100hot list provides a good sample of popular sites. A review of these sites also offers a snapshot of current privacy practices on the Internet today.

ABOUT SECURITY, ENCRYPTION AND SPAM

For purposes of this survey, we decided to examine the collection of personal information and the existence of privacy policies on the Internet. We did not look at the adequacy of security standards, such as whether credit card transactions receive sufficient protection, the availability of good encryption, or the privacy issues related to "spam" (unsolicited commercial e-mail). These are all important issues for on-line privacy and should be examined in a separate study.

COLLECTION OF PERSONAL INFORMATION

One of the first issues we considered was whether personal information is collected at the surveyed web site. For the first part of this query, we were specifically interested in whether the site collected Personally Identifiable Information (PII), such as name or address, directly from the user. We counted email addresses as PII, even though it is possible to spoof an email address and it is not always clear to whom an email address refers.

Many web sites (49 of our sample) collect personal information through on-line registrations, mailing lists, surveys, user profiles, and order fulfillment requirements. However, some web sites, such as CNN, TV Guide, the Washington Post, and the Weather Channel, do not generally collect any personally identifiable information.

We were not able to determine whether web sites are linking data collected on-line with other databases. This classic computer matching technique is oftentimes one of the first indicators of a privacy problem. It is also likely to emerge as a significant issue in the near future. For example, America Online is matching its active member list with demographic and psychographic data obtained from Donnelley Marketing ["America Online Snoops Into Subscriber's Incomes, Children," Privacy Times, May 30, 1997]. We think this issue bears further examination.

PRIVACY POLICY

We were next interested in trying to determine how many web sites actually had privacy policies. Our first conclusion was that finding a privacy policy is not an easy task. We tried a number of different techniques to locate privacy policies.

- We looked at the home page for the term "privacy" with the Find command in the browser software
- We searched the FAQ page for the site for the term "privacy"
- We looked at the legal terms and conditions page for the site for the term "privacy"
- We looked at the customer agreement and similar pages at the site for the term "privacy"

There are other search methods we might have tried, such as running a search engine with the domain name and the word "privacy," but this seemed to us to be beyond the call of duty. We felt that users should be able to locate privacy policies quickly and easily and that a privacy notice should be clear and conspicuous. We excluded privacy policies that were posted to a web site that were actually internal privacy policies for a company and its employees. We found that only 17 of the sites that we visited actually had privacy policies, and few were easy to find.

ADEQUACY OF PRIVACY POLICIES

There are many different privacy policies, but all good policies share certain characteristics: they explain the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary.

For our web survey, we were primarily interested in whether the site told the user why personal information was being collected and how it would be used. If a site didn't make some effort to provide this basic information, we classified it as having an inadequate privacy policy.

Several web sites provided reasonably good privacy notices. Amazon.com, for example, tells users that it does not rent or sell its mailing list to anyone. But Amazon also advises users, "If you would like to make sure we never sell or rent information about you to third parties, just send an e-mail message to never@amazon.com." We thought this statement created unnecessary ambiguity in an otherwise good policy.

Several sites post notices stating that individuals using their sites cannot transmit information that violates privacy, but have no privacy policies themselves.

SECONDARY USE RESTRICTIONS

In examining the few privacy policies that we found, we considered the extent to which users are able to restrict the secondary use of their personal information. Eight of the surveyed sites provide some degree of use limitation. The use limitations are mainly limited to determining whether the collecting organization will be authorized to share (or sell) the information to a third party.

ACCESS TO ONEs OWN DATA

One of the important goals of most privacy laws is to ensure that individuals have the ability to inspect personal information that is collected by others and to make corrections if necessary. This is to ensure that individuals know what information about them is available to others, and also to encourage data collectors to be more forthcoming about how personal information is gathered.

We were interested in finding whether web sites made it possible for users to access the information that the site collected about them.

We couldn't find any site in our sample that currently allows users to access their own file, with the exception of Firefly. The Firefly web site allows users to create a personal profile, to access the profile, and to revise the profile. Firefly provides a good example of user control over a personal profile on the Internet.

ANONYMITY

We were interested in whether users could access sites without disclosing personally identifiable information. Given their nature, we did not look closely at surreptitious techniques that may allow web servers to collect identifying information, such as email addresses or TCIP/IP addresses, from web clients.

We found that every site at least provides access to the home page and most sites let users visit many services on the site without disclosing any personally identifiable information.

We thought the widespread practice of allowing anonymous browsing, even on the most popular web sites, was an important indicator of how privacy is actually protected on the Internet. By avoiding the collection of personal information, web sites encourage users to visit sites. In the physical world, we note that very few stores require the collection of personal information before allowing someone to enter.

We suspect that preserving anonymity may be the easiest way to protect on-line privacy.

COOKIES

There has been a great deal of controversy about the cookies feature in browser software. On the one hand, cookies make it possible for a web server to "recognize" a web client and enables certain features that are useful for surfing and on-line commerce, such as retaining screen preferences, storing passwords, and creating virtual shopping carts.

At the same time, cookies also enable the surreptitious collection of information from the user.

We were interested to see how many of the top 100 web sites enabled the cookies feature. We visited each web site and then checked our cookies file to see if a new line was added. We did not, of course, visit every page or every linked site at each site we visited, so we may have missed some pages that generate cookies.

Of the 100 sites, 24 enable cookies. The cookies feature is often used for registration and password storing, but may also be used to create logs of user interests and preferences (for instance, tracking particular articles that a user accesses at an on-line news site).

We thought it was noteworthy that none of the sites that enabled cookies told the user that information about the user was being placed on the user's system. We think that more could be done to make such transactions "transparent" -- that is to say, readily apparent to the user.

CONCLUSION

Even though privacy is one of the top concerns among Internet users, few webs sites today actually have privacy policies or provide users with information about privacy practices. This makes it almost impossible for users to make informed decisions about their on-line activities.

Many have argued for notice and consent procedures and self-regulation to protect on-line privacy. But a review of the top 100 web sites reveals that only a handful provide any meaningful privacy notice. There is also virtually no indication that any meaningful steps have been taken to protect user privacy by self-regulatory means.

In the absence of meaningful privacy policies, net surfers today also have little assurance that personal information that is provided at a web site might not be misused. Not surprisingly, many users are reluctant to disclose personal information and some provide false information when asked.

Although privacy policies are virtually non-existent on the Internet today, we found that anonymity continues to play an important role in protecting on-line privacy. Many of the top web sites allows users to visit without giving up personal information. Anonymity plays a particularly important role for those sites, such as CNN, that are providing news and information to the on-line community.

It is more difficult to assess how cookies are being used. Sites that have registration or membership, such as Disney or the New York Times, use cookies to store information on the user's system. But other sites enable cookies for purposes unrelated to registration. We don't think users reasonably can be expected to examine cookie files on their hard disks to track cookies usage.

Techniques to provide users with more information about privacy practices, such as eTRUST and other similar branding techniques, should be encouraged. These services should provide clear and meaningful designations for privacy practices. They should also be backed up with regular auditing. We also have doubts about proposed techniques, such as P3, that require users to disclose privacy preferences. We think that good privacy policies should provide meaningful information for users about web site practices and not require users to disclose personal information. Many users are also likely to consider their privacy preferences to be, well, private.

We suspect that one of the simplest and most effective solutions to on-line privacy is to continue the practice of anonymity. Anonymity is already widespread on the Internet -- virtually all of the sites that we surveyed allowed users to use the site without disclosing who they were. When personally identifiable information is collected, web sites should develop clear privacy policies.

RECOMMENDATIONS

Users of web-based services and operators of web-based services have a common interest in promoting good privacy practices. Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of on-line commerce. We also believe it is matter of basic fairness to inform web users when personal information is being collected and how it will be used.

- Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word "privacy."
- Privacy policies should state clearly how and when personal information is collected.
- Web sites should make it possible for individuals to get access to their own data.
- Cookies transactions should be more transparent.
- Web sites should continue to support anonymous access for Internet users.

Protecting privacy will be one the greatest challenges for the Internet. Until clear practices are established and good policies put in place, our advice is simply this: "Surfer beware."

REFERENCES

GVU's WWW User Surveys. One of the best sources for information about the attitudes of Internet users toward privacy issues is the semi-annual survey conducted by the Graphics, Visualization, and Usability Center of the Georgia Institute of Technology. More information about public attitudes toward privacy may be found at the EPIC Privacy Survey page.

OECD Privacy Guidelines. Many privacy policies are derived from the 1980 Guidelines on Privacy and Transborder flows of the Organization for Economic Cooperation and Development (OECD). Other related policies may be found at the International Privacy Documents archive of Privacy International.

EPIC Privacy Archive. The EPIC Privacy Archive contains an extensive collection of documents, reports, news items, policy analysis and laws related to privacy issues.

ABOUT EPIC

The Electronic Privacy Information is a public interest research organization, based in Washington, DC.

Electronic Privacy Information Center
666 Pennsylvania Ave., SE Suite 301
Washington, DC 20003
+1 202 544 9240 (tel) +1 202 547 5482 (fax)
http://www.epic.org/

Mr. COBLE. The gentleman from America's heartland, Professor, it's good to have you with us.

STATEMENT OF PROFESSOR FRED H. CATE, LOUIS F. NIEZEN FACULTY FELLOW, INDIANA UNIVERSITY SCHOOL OF LAW

Mr. CATE. Thank you very much, Mr. Chairman and members of the subcommittee. I appreciate the opportunity to be here.

When I was invited to come today I was asked to address only one question, perhaps in an effort to control my natural long-windedness. That question was: "Does Congress need to take additional action now to protect personal privacy in electronic communications?" My answer is no, and I suppose I could stop there. But, I have four more minutes so let me use that time hopefully wisely.

I'm not suggesting that the extraordinary proliferation of information technologies and services are not presenting important privacy issues or even privacy problems, but rather that further Congressional action in this field at this time is premature and perhaps may be unnecessary altogether. I base that on four considerations, which I will just briefly review.

First, we are in the midst of, not at the end of phenomenal technological innovation that is prompting these new concerns about privacy. Now that to me argues against legislative action at this time, especially in a field such as privacy in which both legislation and judicial interpretations have sought to protect a "reasonable expectation" of privacy. It seems inadvisable to attempt to define a reasonable expectation in the midst of such extraordinary change.

Second, in recent years we have witnessed an increase not only in concerns about privacy, but also in the tools available to consumers to protect that privacy, and in the self-regulatory actions of industries responding to consumer demands. As a result, individuals today have greater opportunities than ever before both to participate in the world around them through the Internet and other digital technologies, but also to protect their privacy while doing so.

And I would just add here that Congress and the Administration should certainly heighten that protection, particularly through allowing high-level encryption, one of the most important technological means of allowing individuals to protect privacy online.

Third, Congress has already provided considerable and valuable protection for privacy, for example, through the Electronic Communications Privacy Act. Congress has also created in citizens and regulators, such as the FTC, further legal rights and legal authority to protect privacy. The FTC, as we already have heard, has focused considerable public attention on privacy issues, it is facilitating the development and enforcement of industry self-regulation and codes of conduct, and it's bringing pressure to bear on companies that are inadequately attentive to consumer privacy issues.

Now I'm not suggesting there may never be a need for legislation to deal with specific information issues, such as children, or sensitive medical information, but rather than the existing authority created by Congress is sufficient to deal with most privacy concerns.

Finally and most importantly I would just take this opportunity to remark that privacy is not an unmitigated good. As the Federal Reserve Board noted in its recent report on financial fraud to Con-

gress "It is the freedom to speak supported by the availability of information and the free flow of data that is the cornerstone of a democratic society and of a market economy."

Protecting privacy inevitably interferes to some extent with the availability of that information and with the free flow of data. Now I believe it is possible and it is certainly desirable to avoid further restrictions on the accessibility of that information by taking advantage of the legal power that Congress has already put in the hands of citizens and regulators and the technological and market power of consumers. These efforts are uniformly preferable in a democratic society to legal restrictions on the collection and the dissemination of information.

Thank you.

[The prepared statement of Professor Fred H. Cate follows:]

PREPARED STATEMENT OF PROFESSOR FRED H. CATE,[1] LOUIS F. NIEZEN FACULTY FELLOW, INDIANA UNIVERSITY SCHOOL OF LAW

SUMMARY

Further Congressional action to protect personal privacy in electronic communications is premature and likely to be unnecessary altogether. That conclusion is based on four related considerations:

1. Rapid Change

First, we are in the midst, not at the end, of the phenomenal technological innovation that is prompting new concerns about privacy. That argues against legislative action, especially in a field such as information privacy, in which past legislation and judicial interpretation have sought to protect "reasonable expectations of privacy." It is inadvisable to define "reasonable expectations" while experiencing such extraordinary change.

2. Expansion of Self-Help and Self-Regulation

Second, in recent years we have witnessed an increase not only in concerns about privacy, but also in the tools available to consumers to protect their privacy and in the self-regulatory actions of industries responding to consumer demands. As a result, consumers today have greater opportunities than ever before both to participate in the world around them and to protect their privacy while doing so.

3. Adequacy of Existing Legal Protection

Third, Congress has already provided considerable protection for privacy and has created in regulatory agencies, prosecutors, and citizens significant legal rights for protecting privacy. The Federal Trade Commission, for example, has been very attentive, especially during the past year, to privacy issues surrounding computerized databases, electronic look-up services, and children's use of the Internet. Although those inquiries are on-going, the FTC, operating under its existing statutory authority, has focused public attention on privacy issues, facilitated the development of industry self-regulation and codes of conduct, identified key principles for meaningful privacy protection, and brought pressure to bear on those companies that are inadequately attentive to consumer privacy issues.

This is not to suggest that there may not at some point in the future be a need for specific, narrowly targeted legislation to deal with privacy issues involving children or sensitive medical information, but rather that existing authority created by Congress is sufficient to deal with most privacy concerns. In short, there is no convincing evidence that new legislation is necessary to deal with privacy issues in electronic communications.

4. Costs of Overprotecting Privacy

Finally, and most importantly, privacy is not an unmitigated good. As a result, efforts to enhance personal privacy should always be evaluated in the context of the

[1] Professor of Law, Louis F. Niezer Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; Senior Counsel for Information Law, Ice Miller Donadio & Ryan. Professor Cate may be contacted at the Indiana University School of Law—Bloomington, 211 South Indiana Avenue, Bloomington, IN 47405, telephone (812) 855–1161, facsimile (812) 855–0555, e-mail fcate@indiana.edu.

costs that those efforts pose to the free flow of information, the development of efficient markets, and the provision of valuable services especially through the Internet.

I am not suggesting that privacy is inherently evil, but rather that it is not inherently good. As the Federal Reserve Board noted in its recent report to Congress on privacy, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy." Protecting privacy inevitably impedes that availability of information and free-flow of data.

I believe that it is possible—and desirable—to avoid further restrictions on the accessibility of information by taking advantage of the legal power that already exists in the hands of citizens and regulatory agencies and the technological and market power of consumers. Efforts by regulators, such as the FTC, and by individual companies and industry groups are further expanding opportunities for meaningful privacy and are helping to inform consumers about the practical steps they can take to control the disclosure of private information. These efforts are uniformly preferable in a democratic society to legal restrictions on information collection and dissemination.

STATEMENT

Mr. Chairman and members of the Subcommittee:

My name is Fred Cate. I am a professor of law, Louis F. Niezer Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington, and senior counsel for information law at Ice Miller Donadio & Ryan in Indianapolis. I am testifying today on my own behalf,[2] as someone who has researched, taught, and written about information law issues generally, and information privacy issues specifically, for more than a decade.[3]

When I was invited to testify today I was asked to address one question: is new Congressional action necessary to protect personal privacy in electronic communications? My answer is "no."

This is not to suggest that the extraordinary proliferation of information technologies and growth in their power and affordability are not presenting important privacy issues, but rather that further Congressional action is premature and likely to be unnecessary altogether. That conclusion is based on four related considerations:

1. Rapid Change

First, we are in the midst, not at the end, of the phenomenal technological innovation that is prompting new concerns about privacy. The World Wide Web, for example, which was first made available to the public in 1992, is now used by more than one-quarter of the U.S. population, making it the fastest-growing medium in human history. By comparison, it took 38 years for radio to reach that percentage of Americans, 13 for television, and 10 for cable. And that dramatic growth is continuing. According to the semi-annual Internet Domain Survey released in January 1998 by Network Wizards, the World Wide Web continues to grow at a dramatic pace. The survey found 29.7 million hosts in January 1998, up from 26 million just six months earlier—a greater than 26% annual growth rate. Five years ago, the survey found only 1.3 million hosts.[4]

The nature of the Internet is changing as well. In 1995, World Wide Web hosts designated ".com" for commercial slightly outnumbered those designated ".edu" for educational institutions—the traditional mainstay of the Internet. The most recent survey, however, shows ".com" sites outnumbering their ".edu" counterparts more than two-to-one.[5] And the disparity may be even greater, because businesses outside of the United States tend to use the abbreviation of their country rather than ".com" as part of their web address.

The fact that we are in the midst of rapid, significant change—not just in technologies but also in the new services, markets, and activities that those technologies

---

[2] In compliance with House Rule XI, clause 2(g)(4), I certify that I have received no federal grant, contract, or subcontract in the preceding two fiscal years.

[3] I am the author of "Privacy and Telecommunications," forthcoming in the *Wake Forest Law Review; Privacy in the Information Age* (Brookings Institution Press, 1997); "The EU Data Protection Directive, In formation Privacy, and the Public Interest," 80 *Iowa Law Review* 431 (1995); and "The Right to Privacy and the Public's Right to Know: The 'Central Purpose' of the Freedom of Information Act," 46 *Administrative Law Review* 41 (1994) (with D. Annette Fields and James K. McBain). A biographical statement is attached.

[4] *See* http://www.nw.com/zone/WWW/report.html.

[5] *See* http://www.nw.com/zone/WWW-9501/dist-byname.html and http://www.nw.com/zone/WWW /dist-bynum.html.

are facilitating—argues against legislative action. This is especially true in a field such as information privacy, in which past legislation and judicial interpretation have sought to protect "reasonable expectations of privacy."[6] It is inadvisable to attempt to define "reasonable expectations" of virtually anything while experiencing such extraordinary change.

2. Expansion of Self-Help and Self-Regulation

Second, in recent years we have witnessed not only an increase in concerns about privacy, but also a parallel increase in the tools available to consumers to protect their privacy and in the self-regulatory actions of industries responding to consumer demands. As a result, consumers today have greater opportunities than ever before both to participate in the world around them and to protect their privacy while doing so.

For example, technological innovations such as adjustable privacy protection settings in both Netscape and Microsoft Explorer, encryption software, anonymous remailers, and in fact, the Internet itself all facilitate privacy and individual control over the information we disclose about ourselves.

Many companies are actively competing for customers by promoting their privacy policies and practices. If enough consumers demand better privacy protection and back-up that demand, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, when competitive markets exist, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much the society really values privacy.

Industry organizations are increasingly providing standards for privacy protection and help to consumers whose privacy interests are compromised. The Direct Marketing Association, for example, operates the Mail Preference Service and the Telephone Preference Service. With a single request to each it is possible to be removed from most DMA-member company mailing and telephone solicitation lists. However, although the Mail Preference Service has been available since 1971, the DMA reports that the service is used by approximately two percent of the U.S. adult population. This suggests that concern over direct mail solicitations is not that great or that the public is unaware of, or not taking the initiative to use, this free service. A proposed use of data can hardly be considered unreasonable if the user gives consumers a meaningful opportunity to object to the use and so few do.

Often, industry associations, such as the Information Industry Association and the Interactive Services Association, have adopted guidelines and principles which may serve as models for individual company policies. Corporate compliance with privacy standards constitutes an increasingly important accolade in competitive markets, particularly among Internet users. Moreover, industry associations can help persuade member organizations to adopt and adhere to industry norms for privacy protection. The DMA, for example, has begun issuing quarterly reports on members who are being disciplined for violating DMA codes of conduct.

A consortium of privacy advocates and software companies has announced the development of a service to make privacy self-help easier on the Internet. "TRUSTe" is a program that rates Internet sites according to how well they protect individual privacy. Internet sites that provide sufficient protection for individual privacy—including not collecting personal information, not disseminating information to third parties, and not using information for secondary purposes—earn the right to display the "TRUSTe" logo.[7]

Considerable privacy protection also exists in private agreements. According to the Bank card Holders of America Association, merchants are prohibited by their agreement with Visa and Mastercard from requiring a driver's license or telephone number for a credit transaction. Similarly, Visa and Mastercard prohibit the merchants with whom they deal from requiring credit card information to guarantee a check. These restrictions create legal obligations through private contracts that help protect individuals' privacy.

3. Adequacy of Existing Legal Protection

Third, Congress has already provided legal protection for privacy in key contexts, such as financial services, and has created in regulatory agencies, prosecutors, and citizens significant legal rights for protecting individual privacy. The Electronic

[6] *See, e.g.*, 15 U.S.C. § 1681e(b) (1997) (Fair Credit Reporting Act of 1970); Restatement (Second) of Torts §§ 652A–652E (1976); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

[7] *See* http://www.truste.org.

Communications Privacy Act of 1986[8] is an excellent example. The Act prohibits the interception or disclosure of the contents of any electronic communication, such as telephone conversations or e-mail, or even of any conversation in which the participants exhibit "an expectation that such communication is not subject to interception under circumstances justifying such an expectation."[9] This language creates significant protection and it is sufficiently flexible to both accommodate new technologies and permit individual states to experiment with greater protection. For example, some states have gone beyond the Act's one-party consent rule to require the consent of both parties if a communication is to be recorded.

Perhaps the best example of the power and flexibility of the current legislative regime is the authority delegated by Congress to regulatory agencies, such as the Federal Trade Commission. In the Federal Trade Commission Act, Congress declared unlawful "unfair or deceptive acts or practices in or affecting commerce"[10] and delegated to the FTC the authority to carry out that provision. Pursuant to that statutory mandate, the FTC has been actively examining privacy issues, particularly in the context of the Internet. The FTC has been especially attentive to privacy issues surrounding computerized databases, electronic look-up services, and children's use of the Internet. Although those inquiries are on-going, the FTC, operating under its existing statutory authority, has focused public attention on privacy issues, facilitated the development of industry self-regulation and codes of conduct, identified key principles for meaningful privacy protection, and brought pressure to bear on those companies that are inadequately attentive to consumer privacy issues.

This is not to suggest that there may not at some point in the future be a need for specific, narrowly targeted legislation to deal with privacy issues involving children or sensitive medical information, but rather that existing authority created by Congress is sufficient to deal with most privacy concerns. In short, there is no convincing evidence that new legislation is necessary to deal with privacy issues in electronic communications.

4. Costs of Overprotecting Privacy

Finally, and most importantly, privacy is not an unmitigated good. As a result, efforts to enhance personal privacy should always be evaluated in the context of the costs that those efforts pose to the free flow of information, the development of efficient markets, and the provision of valuable services especially through the Internet.

The debate over privacy today is fundamentally a debate over control of information. Historically, the United States has accorded enormous protection for privacy through legal respect for private property, which allows individuals to separate themselves from each other; a vigorous First Amendment, which permits individuals the privacy of their own thoughts and beliefs; and unparalleled limits, reflected in the First, Fourth and Fifth Amendments, on government authority to intrude on private property, to compel testimony, or to interfere with practices closely related to individual beliefs, such as protest, marriage, family planning, or worship.

As much protection as U.S. law has offered these and other activities, the law has historically afforded equal protection to the freedom to disclose and disseminate information about such activities. This freedom is at the core of the First Amendment. It is also at the core of a market-based economy, which depends on the accessibility of information.

While privacy is certainly a necessary element of quality life in modern society, protecting the privacy or information imposes real costs on individuals and institutions. Privacy facilitates the dissemination of false information, such as when a job applicant lies about his previous employment, by making discovery of that falsity more difficult or impossible. Privacy similarly protects the withholding of relevant true information, such as when an airline pilot fails to disclose a medical condition that might affect job performance. Privacy interferes with the collection, organization, and storage of information on which businesses and other can draw to make rapid, informed decisions, such as whether to grant credit or accept a check. As these examples suggest, the costs of privacy may be high. Those costs include both transactional costs incurred by information users seeking to determine the accuracy and completeness of the information they receive, and the risk of future losses resulting from inaccurate and incomplete information. Privacy therefore may reduce productivity and lead to higher prices for products and services.

Privacy recognizes the right of the individual, as opposed to anyone else, to determine what he will reveal about himself or herself. As a result, privacy conflicts with

[8] 18 U.S.C. §§ 2510–2520, 2701–2709 (1997).
[9] *Id.* §§ 2510–11.
[10] 15 U.S.C. § 45(a)(1) (1997).

other important values within the society, such as society's interest in facilitating free expression, preventing and punishing crime, protecting private property, and conducting government and commercial operations efficiently.

To the extent that legal protections and social mores concerning privacy interfere with creating the systems necessary to acquire and use personal information, privacy may even conflict with the interest of the persons whose privacy is being protected. If a customer wants credit in a retail store, but the law prohibits the store owner from obtaining or verifying the credit information necessary to extend that credit, the customer is inconvenienced, even though he or she may be willing at that moment and for that purpose, to consent to the disclosure of his or her credit information. If an individual requires emergency medical attention, but privacy laws interfere with the hospital obtaining his or her medical records, he or she may face greater risks than mere inconvenience. Instant credit, better targeted mass mailings, lower insurance rates, faster service when ordering merchandise by telephone, special recognition for frequent travelers, and countless other benefits come only at the expense of some degree of privacy.

I am not suggesting that privacy is inherently evil, but rather that it is not inherently good. The late Anne Branscomb, author of Who Owns Information?, wrote: "Information is the lifeblood that sustains political, social, and business decisions."[11] This is especially true in commercial contexts where, as the Federal Reserve Board noted in its recent report to Congress on privacy, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[12] Protecting privacy inevitably impedes that availability of information and free-flow of data.

This is particularly true in the context of laws affecting electronic communication. The vast majority of information in the industrialized world today is electronic. No form of communication other than face-to-face conversation and hand-written, hand-delivered messages, escapes the reach of electronic information technologies. As those exceptions indicate, no communication that bridges geographic space or is accessible to more than a few people exists today without some electronic component. And the dominance of electronic communication is growing at an astonishing pace.

As a result, the regulation of electronic information flows cuts deeply into freedom of expression and the data necessary for open markets generally. And the dangers inherent in limiting the flow of information are exacerbated by the rapidly expanding and changing context in which information is created, transmitted, stored, and used. Such restrictions should be avoided if possible.

I believe that it is possible—and desirable—to avoid further restrictions on the accessibility of information by taking advantage of the legal power that already exists in the hands of citizens, prosecutors, and regulatory agencies and the technological and market power of consumers. Efforts by regulators, such as the FTC, and by individual companies and industry groups are further expanding opportunities for meaningful privacy and are helping to inform consumers about the practical steps they can take to control the disclosure of private information. These efforts are uniformly preferable in a democratic society to legal restrictions on information collection and dissemination.

These measures may be fully effective in protecting privacy to the extent compatible with a democratic society and market economy. Or it may ultimately prove necessary to enact additional laws to strengthen privacy protection. I do not believe that is the case today in the face of expansive change, impressive technological and commercial alternatives for protecting privacy, powerful existing law and regulators, and strong constitutional preference against such restrictions.

Thank you.

BIOGRAPHICAL STATEMENT

Fred H. Cate is a professor of law, Louis F. Niezer Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington. An internationally recognized expert on information law, Professor Cate is also senior counsel for information law in the Indianapolis law firm of Ice Miller Donadio & Ryan.

Professor Cate is the author of many articles and books, including *Privacy in the Information Age*, which received Honorable Mention as the Association of American Publishers Professional/Scholarly Publishing Division Best New Book in Law 1997,

[11] Anne W. Branscomb, "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985, 987 (1983).

[12] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (March 1997).

and *Sexually Explicit Expression in the Classroom: The Internet, Schools, and the First Amendment*, and he is the editor of *Visions of the First Amendment for a New Millennium*.

Professor Cate chairs the American Association of University Professors' Intellectual Property Committee, and he serves as a member of the U.S. Privacy Experts Group, the Privacy Exchange Advisory Board, and the Committee on Institutional Cooperation's Copyright and Intellectual Property Committee. He is secretary of the Board of Directors of the Advanced Research and Technology Institute and faculty advisor to the *Federal Communications Law Journal*, the official journal of the Federal Communications Bar Association and the nation's oldest communication law journal.

Previously he directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the Department of Health and Human Services' Working Group on Intellectual Property in Networked Health Information, and served as a member of the U.S. Congress Office of Technology Assessment's panel of experts on Global Communications Issues and Technology and panel of reviewers on International Money Laundering. From 1990 to 1996, he served as a senior fellow (and from 1991 to 1993, director of research and projects) of The Annenberg Washington Program in Communications Policy Studies.

Professor Cate writes widely for the popular press—including the *Atlantic, Chicago Tribune, Christian Science Monitor, International Herald Tribune, Los Angeles Times, San Francisco Chronicle, Wall Street Journal*, and *Washington Post*—and has appeared on CNN, PBS, and many local television and radio programs. He received his J.D. and his A.B. with Honors and Distinction from Stanford University. Prior to joining the faculty at Indiana University, he practiced in the Washington, D.C. office of Debevoise & Plimpton. A life member of Phi Beta Kappa Associates, Professor Cate is listed in *Who's Who in American Law*.

He can be reached at: Indiana University School of Law—Bloomington, 211 South Indiana Avenue, Bloomington, Indiana 47405, telephone (812) 855–1161, facsimile (812) 855–0555, e-mail fcate@indiana.edu.

CSI Coalition of Service Industries ■ Research and Education Foundation

Conference on Fair Information Practices and Data Privacy: How We Got Here, Where We're Going

An Intensive Briefing by Experts In the Data Privacy Field

Fred H. Cate, Conference Chair*

April 16, 1998
12:30 p.m. to 5 p.m.

Fifth Floor Auditorium
The National Museum of Women In the Arts
1250 New York Ave. Northwest
Washington D.C.

Statement of Purpose

"Privacy" is among the most hotly debated topics in Washington and other national and state capitals today. This surge in attention is largely driven by the proliferation and power of the World Wide Web and other information technologies and by the looming October effective date of the European Data Protection Directive. As a result, debate over privacy protection is often characterized by its focus on the novelty of the issues involved and by the extent to which U.S. privacy protections meet European standards.

Yet many privacy issues are not new; they have been the subject of extensive discussion and review in the United States for at least 25 years. And the resulting combination of sectoral regulation, self-regulation, and self-help measures reflect a distinctively U.S. context and important U.S. values.

Whatever the arguments for action today, that action should be informed by the history and context of the privacy debate in the United States. "How We Got Here-Where We're Going" will provide a half day, wide-ranging overview of the privacy debate in the United States, a survey of key milestones in the evolution of the current regulatory structure, an examination of important and often overlooked principles that undergird that structure, and specific, practical insights on future steps in U.S. privacy protection.

805 15TH STREET, N.W. ■ SUITE 1110 ■ WASHINGTON, DC 20005 ■ (202) 289-7460 FAX (202) 775-1726

AGENDA

Panel I
12:30 p.m. to 1:30 p.m.

I. Character of U.S. Information Economy
- Vast, Open Public Record
- Long History of Shared Private Data
- Freedom of Expression

Marty Abrams, Vice President Information Policy & Privacy, Experian

II. Assuring Consumer Rights
- A System of Multiple Checks & Balances with Many Players
- Assuring Appropriate Information Use

Peggy Haney, Vice President Consumer Affairs, American Express

III. Fair Credit Reporting Act
- Establishing a System Based on Preventing Harmful Use

John Ford, Vice President Privacy and External Affairs, Equifax
Mallory Duncan, Vice President, General Counsel, National Retail Federation

Panel II
1:30 p.m. to 2:30 p.m.

IV. Development of Fair Information Practices
- HEW Department's Groundbreaking Efforts
- The Concept of the Consumer as Exerciser of Access Control

Russell Pipe, Deputy Director, Global Information Infrastructure Commission (Invited)

V. U.S. Privacy Act - Applying Fair Information Practices Principles to Federal Government
- Applied Only to the Federal Government
- Preventing Abuse by Government Key Purpose

Ron Plesser, Attorney at Law, Piper Marbury

VI. Genesis of European Data Protection & OECD Guidelines
- Layer of Explicit Government Control - Data Commissioners/Registrars
- Weak Implementation of OECD Guidelines

Charles Prescott, Attorney at Law, International Business & Law

Coffee on the Mezzanine
2:30 p.m. to 3 p.m.

Panel III
3 p.m. to 4 p.m.

VII. EU Data Protection Directive
- Globalization of Standards, or Emphasis on Process?

Jim Maxeiner, Vice President & Associate General Counsel, Dun & Bradstreet

VIII. U.S. Administration's Framework for Electronic Commerce
- OMB Working Group Privacy Principles
- Focus on Transparency, Consumer Education and Consumer Choice

Becky Burr, Senior Internet Policy Adviser
National Telecommunications & Information Agency, Department Of Commerce

IX. Enforcement Models from Federal Law
- Section 5 FTC Act

David Medine, Associate Director Credit Practices
Bureau of Consumer Protection, Federal Trade Commission
Christopher Wolf, Attorney at Law, Proskauer Rose L. L. P.

Panel IV
4 p.m. to 5 p.m.

X. Contracts to Facilitate Cross Border Data Flows

Scott Blackmer, Attorney At Law, Wilmer, Cutler & Pickering (Invited)

XI. Can Technology Supply the Answer?
- Feasible/"Technology Modalities"

Marilyn Cade, AT&T (Invited)

XII. What Is "Adequacy," Defining the Common Denominator
- Systems for Assuring Appropriate Information Use

Fred Cate, Director, Information Law and Commerce Institute
Indiana University School of Law

Mary J. Culnan, School of Business, Georgetown University

REGISTRATION FORM

FAIR INFORMATION PRACTICES AND DATA PRIVACY: HOW WE GOT HERE, WHERE WE'RE GOING

AN INTENSIVE BRIEFING BY EXPERTS IN THE DATA PRIVACY FIELD

Fifth Floor Auditorium
The National Museum of Women in the Arts
1250 New York Ave., NW, Washington, DC
April 16, 1998

12:30 p.m. to 5 p.m.

$40 Fee

Sponsored by the
U.S. Coalition of Service Industries Research & Education Foundation

To reserve a place at the Information Practices/Data Privacy Conference, please complete the form below and fax to Program Manager Linda Schmid at (202) 775-1726. You may also call (202) 775- 7459 for answers to immediate questions.

Name: _____

Organization: _____

Address: _____

Telephone: _____ Fax: _____

E-mail: _____

Please make checks payable to:

Coalition of Service Industries Research & Education Foundation*
805 15th Street, NW, Suite 1110
Washington D.C. 20005
Attention: Linda Schmid

*The Coalition of Service Industries Research & Education Foundation is a tax exempt, nonprofit 501(c)(3) foundation

Mr. COBLE. And you beat the red light, Professor.

Thank you all for being with us.

Professor, in your written testimony you alluded to a program that rates Internet sites according to how well they protect individual privacy. Does that service also work with sites that do not rate so well on methods privacy protection?

Mr. CATE. Well, Mr. Chairman, I think the value of an organization, and I think I was referring in my testimony to Truste, the value of that type of rating is to provide a sort of consumer seal, a Good Housekeeping Seal, if you will, so that people who use the Internet when they visit a site will know that this site has been rated by some organization as meeting the standards of that organization. Presumably the alternative is that if you find a site that does not bear that Truste symbol you might be hesitant, I would be hesitant, to then provide data or information to that site without specifically inquiring into its privacy policies.

Mr. COBLE. Mr. Rotenberg, some insist and perhaps justifiably so, that in this rapidly advancing Internet environment in which we live that any legislation enacted by government or the Congress would be obsolete shortly after its passage. How do you respond to that contention?

Mr. ROTENBERG. Mr. Chairman, I think it's a fair concern, but we've wrestled with this issue before. You know, in the '60's the Federal Government was introducing computers across the government and was raising great privacy concerns, and it took a lot of time, but by 1974 we passed the Privacy Act and put in place fundamental Fair Information Practices, and that law stood the test of time. In 1980, the OECD in Europe got the leading industrialized nations together and said we need a set of principles to protect privacy, and those set of principles have been in place for 20 years. I think it can be done. I don't think technology should make us back off. But more importantly I think the American public today wants it to be done. They want privacy protection on the Internet and they don't want to wait.

Mr. COBLE. Ms. Mulligan, you indicate in your testimony, you support the creation of a privacy entity whose expertise could be utilized when addressing policy recommendations on privacy issues. Administratively how would such an entity operate and who would run it?

Ms. MULLIGAN. These are good questions. I think that it's important to create such a structure, and I think that the creation of such a structure would need to be very well thought through. I think there are certain components. One thing would be independence, it is really crucial to the functioning. If you look at Administration policies on encryption and if you look at the recent recommendations coming out of the Office of Health and Human Services on privacy protections for medical records that contained no constraints on law enforcement access to health data you can see that there is no independent focus on privacy. There is no strong privacy voice within the Administration. I think that such an office would have a role in commenting on legislative proposals, making recommendations, and providing experience and a forum for discussion, such as the Federal Trade Commission has had over the past 3 years. I have focused more on the functions that such an agency

would provide or an entity would provide rather than on having a blueprint of exactly what its structure would be.

Mr. COBLE. Professor, I, too, won the race with the red light you will note. [Laughter.]

The gentleman from Massachusetts, Mr. Frank.

Mr. FRANK. Thank you, Mr. Chairman.

Let me ask, Professor Cate, because I certain agree we should not think that privacy is the only value, although I will have to say if I were citing someone who was critical of excessive privacy I probably wouldn't use the Federal Reserve because until very recently they believed in secrecy for themselves. It was only after the prodding of our colleague, Mr. Gonzalez that they decided that they could announce on the date that they voted to raise interest rates that they had done so. They used to have to wait. They do now grudgingly make their minutes available weeks after they happen. So I agree with you in principle, but let me say this. If you were trying a case you wouldn't put them on the stand to be your privacy advocate. They would be rather easily impeached.

Beyond that, and I agree with much of what you said, but I do have some questions about it. Let me ask you, for example, the FTC under its unfair and deceptive authority is going to try to protect children. Should a court say they can't do that, would you then be in favor of our legislating?

Mr. CATE. Yes, I would, sir.

Mr. FRANK. Okay. You know, I'm ready to see how far they can go. I would say this, and that's your red light, or Howard's red light, not mine I just want to be clear [Laughter.]

I understand the need to be flexible, but two issues. One, what about adults, and I think this is the policy question. Do adults have a right, do they have a reasonable expectation, and should it be enforced by law, that information they give for purpose "a" will be used only for purpose "a" and not for a lot of other purposes?

Mr. CATE. Well, Congressman Frank, I think that depends on whether they are told that it will only be used for that purpose.

Mr. FRANK. I understand that, but what if they're told nothing? I think in the majority of cases in my experience you are told nothing. You are not told it's going to be used and you're not told it's not going to be used. You're told $18.37, $246, this is how much it cost, here is my credit card number, thank you very much, and that's the end of it. I mean obviously if you're told and you give it to them, that's one thing, unless you're a child, and we agreed to deal with that. If you're told that they won't use it, and they use it, then there is an unfair practice. But what about that great bulk of cases where nothing is said on the subject of what's going to be used?

Mr. CATE. If nothing is said, then I believe the use should be unlimited.

Mr. FRANK. Would you put any obligation of notification to the consumer?

Mr. CATE. I would not put an obligation of notification under the current structure. I will say in other settings I have advocated legislation that would require organizations to disclose what their privacy policy is.

Mr. FRANK. When you say organizations to disclose it, I mean transaction by transaction or in general?

Mr. CATE. I think in general.

Mr. FRANK. But not transaction by transaction?

Mr. CATE. Not transaction by transaction, right.

Mr. FRANK. I might as well save our time. I mean we're talking about people who are engaging in transactions. So I guess that's the policy question, and I must say I don't think frankly the current state of the evolution of technology will directly bear on that. There is a principle here. Do you have a right to be told that the information that you give out, and maybe it's some information and not others, is going to be used, your Social Security number or other things, for other purposes, and I guess that may just be a substantive disagreement, because I do think within an organization, corporation, whatever it is, publishing information practices is not very useful.

The other question I have though is, you know, and let's be very clear, we do agree that there has to be a legal basis, and the question is whether it should be I think a specific or a general one. Government can't go act and the Executive Branch people can't just go act without there being an ultimate statute. And I wonder from the standpoint of businesses, and right now what we've got is the Federal Trade Commission, a Federal regulatory body not directly controlled by the Executive, and their mandate is "unfair or deceptive acts or practices." That's pretty broad. I mean do you have confidence that that's the best way to deal with this, to let the appointed members of the FTC decide what content to give to that?

Mr. CATE. I have confidence that that's the best way to proceed at this moment. It's a regulatory body in place, its powers are fairly well defined by statute and by the courts, it's an entity with which organizations are used to dealing, and it's an entity that——

Mr. FRANK. Yes, it was well defined——

Mr. CATE [continuing]. Has muscle in dealing in this area.

Mr. FRANK. It's well defined under the old rules, but you say we've got this whole new technology, and I've got to say I don't get a lot of guidance from unfair or deceptive in the privacy area. I mean deceptive is fairly easy, but what's unfair in the privacy area, and I think simply letting the FTC Commissioners decide that is a problem.

Mr. Rotenberg.

Mr. ROTENBERG. Mr. Frank, if I could pick up on that point. I think, you know, certainly the FTC should get some credit for trying to address privacy issues, but the FTC was never intended really to address these kinds of issues. That particular policy, Section 5 of the Federal Trade Commission Act, goes to issues related to advertising, and one of the very——

Mr. COBLE. Mr. Rotenberg, I didn't hear you. You said the FTC was not very attentive in what? I didn't hear what you said.

Mr. FRANK. Was not intended to do privacy.

Mr. ROTENBERG. Not intended to do privacy. You know, there has been only one opinion in the now 3 years that they've been looking at privacy issues, a three-page opinion of staff on a case that was already rendered moot because the company discontinued the practice prior to when the decision was rendered. So there is a question

actually about the adequacy of enforcement. But there is a very peculiar disincentive in this current regulatory structure. You see, if you're going to go after people in the privacy world for unfair or deceptive statements, you know, we say we do "a" but we end up doing "b"——

Mr. FRANK. Let's just talk about unfair because I think deceptive is easier. I think the real issue here comes in where you give this agency this roving mandate of unfairness, and let's just restrict it to unfair.

Mr. ROTENBERG. Well, fine, unfair. So I say to you I'm going to do "a" but I end up, you know, doing "b", and the FTC says well that's unfair, they didn't think that the information was going to be disclosed, and the company says you're right, you know, I shouldn't be telling people that I'm going to do "a" if I end up doing "b". So, guess what, everyone who is intending to do "b" does "b" and people are very careful about promising "a", which may very well be what people want because they're going to get caught not following the policy they——

Mr. FRANK. Well, see, I think the issue is deceptive takes care of saying one thing and doing another, but unfair does not.

I would ask for another minute, Mr. Chairman.

Mr. COBLE. Without objection.

Mr. FRANK. You know, I worry from the democratic standpoint and from the standpoint of, you know, businesses tell us we would like some certainty. If all we've got is a general mandate to the FTC, and Mr. Rotenberg's point is absolutely right. I don't think Woodrow Wilson had the Internet at the forefront of his mind when he was thinking about this or privacy, as much as Brandice might have been involved in both aspects. I think the FTC was not, that this was not the right to be let alone part, but this was the right to go be actively interfering, and it's a pretty thin read it seems to me in democratic theory to give the FTC this mandate to deal with unfairness.

Ms. Mulligan.

Ms. MULLIGAN. I think there are some areas that the Federal Trade Commission might explore in looking at unfair. For example, if you look at the Kids.com staff letter where they found unfair is where there was a potential for harm that was unreasonable, and I actually filed a complaint about two web sites that were collecting sensitive health information from people, and I was concerned that——

Mr. FRANK. I don't think children.

Ms. MULLIGAN. Adults, and I was quite concerned that they were not necessarily telling people how they were going to use that information. And because of the sensitive nature of that information, and we're talking about information about serious illnesses, I think the disclosure of that information to people in ways in which those people had no knowledge could in fact be quite unfair and cause harm.

Mr. FRANK. I agree, and let's be very clear again. Apparently there was no deception involved. They didn't say tell us this and we'll never tell anybody.

Ms. MULLIGAN. Well I think there could both.

Mr. FRANK. No, excuse me. You know, words, it's a good thing that we have different words for different things because the more a word means the more ambiguity and lack of clarity we're going to have in having a discussion. The reason I say that is it's a slippery slope. Everybody against deception, or it's at least easier to define deception. Let's take the case of some people who were not deceived. Nobody said I'm going to find all about your health and I'm going to sell it to somebody. They didn't say I'm not going to do it and it wasn't deceptive. You're saying it's unfair in some cases to get this health information and then sell it to other people or use it for other purposes?

Ms. MULLIGAN. I certainly think that if, for example, somebody was running a web site that was collecting information, and they weren't making any disclosures about how they were going to use that information, but a consumer came there and it was an insurance site, for example, and they thought they were finding out about insurance premiums, and in fact somebody was taking that information and disclosing it to people who were going to deny them insurance or to employers in their area, I think you could make a strong case that that's harm and that that could be unfair.

Mr. FRANK. Well we had something that seemed to me to come maybe within that ambit when we had the pharmacies selling prescription information. Now in some cases they said they were going it for the goodness of our hearts, you know, that maybe I forgot to take my pills and this very nice druggist was going to call me up and say, hey, you didn't take your pills, and that was very nice of them, but I don't think that was the only motivation. And that again is not deceptive, or at least if it's deceptive it's implicitly deceptive. You can create an impression that it's going to be for this purpose, and then you sell it for another purpose.

I guess the question is should we leave it up to the FTC on a case-by-case basis to decide what is unfair or not, and I think there was going to be some obligation for us to deal with a kind of threshold principle. Are adults who are of sound mind being deprived of a legal right if they give information for what they assume to be one purpose, but it turns out to be that there is some other purpose that they find invades their privacy, and I don't know how you leave that to the FTC simply to decide whether it's unfair or not as a general principle.

Ms. MULLIGAN. May I?

Mr. FRANK. Yes.

Ms. MULLIGAN. I think the Administration has put forward this idea that self-regulation can work and that "there will be a market for privacy practices," and I think if there is going to be any consumer protection that is based on a market analogy you have to meet the prerequisites for a market, fair information, full information and bargaining power. I mean there are a lot of threshold issues, and I think you're right, I think without disclosures about what the practices are the model doesn't work.

Mr. FRANK. Right, and I understand the market, but I mean what's the market if my problem is that somebody gets this information from me and sells it, and how do I buy privacy. I mean, you know, do I send some guys from Reviere over to talk to them? I don't understand what's the market.

Ms. MULLIGAN. I was trying to answer your question as to whether or not FTC enforcement works or not.

Mr. FRANK. I understand that, and this is not a test, Ms. Mulligan. I'm trying to expand on the thing, and I'm saying that I understand your point, and I think there is a real problem with the market, and in particular there is a problem with the market when I don't even know I'm in the market because I don't know that they have used my data for this reason. See I think to respond to a point my colleague mentioned before, I think we're getting the complaints about violations of privacy from people who don't understand where it came from. People are objecting to things that they get, solicitations, et cetera, et cetera, without realizing that this may have come from their having volunteered information in one context which was used in another.

Mr. Rotenberg.

Mr. ROTENBERG. I just want to say that your point that unfairness is too vague and we don't want to leave it to the FTC to sort all that out is absolutely right, not only because of the term itself, but also because we have a lot of history and a lot of understanding with fair information practices which really are widely talked about and widely understood by U.S. companies and by other countries, and we need to be focusing on those principles. Limiting the secondary use, which is what you're talking about, is central to that. I don't know what unfairness means.

Mr. FRANK. There is one last point I want to make, and that is I understand we have rapidly evolving technology, but that may be a reason to act because there is that metaphysical principle that quantity can become quality, that if you in fact radically alter the quantity of things you can do you are changing the quality to some extent. I say that because some of these issues that were not necessarily problems when it had to be done by hand can become problems as the efficiency of the information gathering and information dissemination is qualitatively increased, and that's why the very fact that we're dealing here with technology means that some of these old principles may not work.

I guess one final example is this Congress voted to ban phone calls that were automatically dialed, but not phone calls in the same circumstance that were made by individuals, and the reason was that the availability of the computer-dominated machinery changed that operation, and we were ultimately, although there was initial court decision, no, I believe that has been upheld by the courts. So that was a case where the introduction of technology, there is something that is okay to do, and it has to do with invasion of privacy and calling people in their homes, it's okay if it's not done with the great technological sophistication, but it's illegal if it is.

Thank you for your indulgence, Mr. Chairman.

Mr. COBLE. You're indeed welcome, Mr. Frank.

The gentleman from Virginia, Mr. Goodlatte is recognized for 5 minutes.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. Cate, I also want to follow up on Mr. Frank's line of questioning regrading the area of government involvement in protecting privacy on the Internet because I certainly agree that there should

be a go slow approach to the government getting involved there, and I also agree with your statement that a right to privacy is not an absolute. There are instances where the interest of society intervening and invading somebody's privacy for the purpose of preventing a crime or otherwise protecting the public good is justified.

I know where Ms. Mulligan and Mr. Rotenberg stand on my legislation regarding current government policy interfering with one's right to protect one's privacy on the Internet and my legislation attempting to change that policy regarding encryption, and I wonder what your views are on that?

Mr. CATE. I think you will be satisfied with my views on this, sir. I strongly support encryption availability and I support your bill in that regard.

Mr. GOODLATTE. There are three for three then.

Mr. CATE. Let me just say, if I may, in this sense I completely agree with Marc Rotenberg. There is no question but what government has got it wrong by on the one hand saying we want to focus on self- regulation and so forth, which I support, but on the other hand saying we want to bind your hands when you use the tools that make self-help available, namely, encryption, one of the most important of those tools. I don't think you can have it both ways.

Mr. GOODLATTE. Thank you.

Mr. Rotenberg, Ambassador Aaron talked about not mandating encryption, but as Mr. Rogan quoted from his written testimony, if private industry efforts failed the government would get involved, and I wonder if you want to comment on some of those things that are short of actually having a mandatory key recovery system as prescribed by the Director of the FBI, Mr. Freeh, and truly having a totally voluntary key recovery system, which I have no problem with. If individuals want to have someone else hold the key to their computer because it contains their financial records, their business records or whatever the case might be, and they lose their own access to the computer and they want to be able to have somewhere else they can go to get that access, I have no problem with that at all, but that is not what I understand the Clinton Administration to be talking about, and I wonder if you might comment on that yawning gap between where I stand and where the Director of the FBI stands.

Mr. ROTENBERG. Well it's an excellent point, Mr. Goodlatte. The Administration is fond of saying that they support market-based solutions in the encryption realm, but these are market-based solutions as long as they meet the government's requirement, and short of passing law what we are seeing is the continued enforcement of the export control regime which tells U.S. companies that you're not going to sell products outside of this country unless you design them in a way that meets the government requirements.

A tremendous amount of money I should point out, sir, is being spent within the Federal Government by Federal agencies to try to make key escrow work, and it may be appropriate at some point to actually look at what is coming out of that. There is the continued pressure and arm twisting on U.S. industry and even individual cryptographers to try to come in line with the Administration's policy. And finally, as you mentioned at the outset, the *New York Times* story about the international survey of cryptography policy,

and that is a survey that was done in our office by Mr. Wayne Madsen, who is here this morning. What we found when we did that survey, and it was I believe the most comprehensive survey done to date, is that other countries are not going down this path. They want to promote electronic commerce, they want good encryption, and like you said they recognize that there are law enforcement concerns and they want to address them, but they don't want to restrict the development of encryption in this manner.

Mr. GOODLATTE. Ms. Mulligan, do you believe that export controls on encryption are effectively domestic controls on encryption?

Ms. MULLIGAN. I think the impact of export controls has been to severely curtail the availability of strong encryption in this country, and I think importantly, if you listened to what Ambassador Aaron said earlier, I think his comments basically told us that rather than exporting democracy we're trying to export our surveillance system to the rest of the world, and I don't think you can have a policy that meets that goal and not having an impact on what's available domestically. So, yes. I mean I think if anything what we know is that this is global medium and our export controls are going to have a severe impact on what is available domestically.

Mr. GOODLATTE. Mr. Rotenberg, would you elaborate on your comments about efforts being made within the Administration to develop key recovery systems. It's my understanding that includes proposals to require that individuals doing business with the Federal Government and to electronically communicate with it must use a system that includes a key recovery feature in it.

So that, for example, if at some point in the not too distant future virtually everyone in the country filed their tax returns electronically with the Federal Government, even though they weren't mandating a key recovery system on anybody who wanted to buy something other than that, if effectively your means of communicating with the outside world, including filing your tax return with the Federal Government, required you to use a key recovery system that complied with their standards, would we be mandating key recovery?

Mr. ROTENBERG. Well this is another reason, sir, why we tend to put quotation marks around the word "voluntary" when describing the Administration cryptography policy, and the filing of IRS records is a good example. The Administration is in negotiations with the Department of Treasury to try to get support for a key escrow encryption requirement for taxpayers, and the Treasury Department, like other Federal agencies, is resisting because of very practical and well-understood problems. There is cost, there is risk, there is overhead and there are the privacy concerns associated with key escrow. But of course, you can say well you don't have to use key escrow, but if you intend to submit your tax return, as you're required to do by law, then you'll need to use it.

Mr. GOODLATTE. Using a system where the key will be stored by the government for potential future use.

Mr. ROTENBERG. Right. Well as I mentioned earlier, the routine uses of cryptography, changing a user ID on your account, buying a book online, are so common place and so much a part of everyone's experience of the Internet that the thought that the key that

is generated for each one of those transactions has to be saved and stored and accessible by law enforcement because it may somehow be necessary in a criminal investigation makes almost no sense. I'm sure at some point somewhere cryptography is going to create a problem for law enforcement, but if to respond to that every one of those transactions online is going to be escrowed the Internet will just never take off.

Mr. GOODLATTE. Mr. Chairman, I wonder if I might have two additional minutes.

Mr. COBLE. If you can please move it along. Go ahead.

Mr. GOODLATTE. Thank you.

I just want to ask Mr. Rotenberg and Professor Cate if they have any knowledge of the cost of such a key recovery system. You mentioned it in passing there. It's my understanding that we have about 1,100 wiretaps that are authorized by the courts in this country in an average year to all law enforcement agencies, not just the FBI, but State and local law enforcement as well. The vast majority of those are to tap into telephone communications in the future, and perhaps there are a few today where they're tapping into some other forms of communications that might utilize encryption, but comment on what percentage of those now and in the future are likely to have encryption attached to them and divide that into the estimated cost. I have heard it estimated that a key recovery system mandated on the entire country could cost billions of dollars a year, and what are we talking about in terms of the cost per wiretap for law enforcement to be assured that they have this means of decoding communications. As I indicated earlier, there are a lot of other means that they can get access to the same information, but assuming that this is what they absolutely feel they have to have what are we talking about per wiretap in terms of the cost?

Mr. ROTENBERG. Let me say, Mr. Goodlatte, I can give you a fairly specific answer on the wiretapping issue because we actually track that question. We monitor how much Federal wiretapping occurs and what the costs are to the Federal Government, and I think in 1996 it was about $57,000 per wiretap. The question which you're asking now though concerns what happens——

Mr. GOODLATTE. If we go to aid that wiretapping by a mandatory key recovery system.

Mr. ROTENBERG. Yes, I understand that, and what I would like to do if it's acceptable to you and the subcommittee is actually provide some information to the subcommittee after the hearing when we've had a chance to do that research. I think the costs are going to be extraordinary, and I say this because current wiretapping costs are associated with those related to a specific investigation, the agent's time, the equipment used and the target on the criminal suspect. Key escrow is based on a very different approach. It is based on reconstructing the entire communications network.

You know, there is a related discussion taking place right now about the cost of implementing the communications assistance for the Law Enforcement Act. $500 million was authorized for that program, an extraordinary figure, and doesn't even begin to approach the actual costs likely for industry that are going to result in trying to implement it. So we are talking about orders of mag-

nitude between the $50,000 per wiretap today and the hundreds of millions of dollars, billions perhaps, to try to implement key escrow.

Mr. GOODLATTE. And per wiretap in the millions and perhaps even tens of millions of dollars per wiretap?

Mr. ROTENBERG. Yes, possibly.

Mr. GOODLATTE. We would like to have that information, Mr. Chairman, if it is possible for them to provide that.

Mr. COBLE. I think that would be in order.

Folks, let me think aloud a minute. I am not going to affix muzzles to the chins of the gentleman from Massachusetts nor the gentleman from Indiana nor the witnesses, but the cloak room advises me that a vote is imminent. I think we will all benefit if we could wrap up. So, if you can keep your answers terse we would be appreciative. I am pleased to recognize the gentleman from Massachusetts.

Mr. DELAHUNT. Mr. Chairman, I will take your admonition seriously.

Mr. COBLE. There is no threat intended at all there, Bill.

Yes, Ed.

[Congressman Pease informs the chairman he has to leave.]

Well Mr. Pease has to leave us anyway. I don't want to run you away, Ed. But I think we'll all benefit if we could wrap it up.

Go ahead, Bill.

Mr. DELAHUNT. Professor Cate, there is an interesting conflict here because you say there is no need for Congressional action and you hope that self-regulation can accomplish what we need in terms of privacy protection, and yet if you listen to the wise words of Congressman Goodlatte on this issue and what we have heard from the industry, the answer, if it's going to be in the technology, is being inhibited by Administration policy. Do you agree?

Mr. CATE. Well let me clarify, and I will do so very briefly. First, I was not suggesting that self-regulation is enough. I was saying that in the existing laws that are already passed and the availability of technologies that are available to consumers and self-regulation, that is enough at the moment. If the way the Administration is going to implement those laws to deny access to those tools, then Congress will need to act to make those tools available to the public.

Mr. DELAHUNT. You know my friend from Massachusetts, Mr. Frank, talked about unfairness, but my memory of a course in law school was that unfairness related to the issue of advertising. I mean when we talk about unfairness and the use of the word deception, I don't know if it does apply. It's almost as if it were a misappropriation, if you will, of a piece of my privacy or your privacy or anybody's privacy, and that's what we're really talking about here. And I guess you can't really describe it as a theft because the real problem is that we don't know.

When I asked Mr. Medine or maybe it was Ambassador Aaron, there is no data, there aren't any studies that they were aware of at least that could define or measure the problem. We just don't know, but we know that in cyberspace, or however you want to describe it out there, there is a real concern. It's a dilemma, it's a real dilemma. Comments.

Mr. CATE. I would just like to say, sir, I agree with that, but let me point out that nine million new businesses went online in the past 6 months and opened new web sites. It is an evolving set of issues and behaviors, and we're seeing a dramatic change in who populates the Internet and what services are there. It's unreasonable to talk about the Internet as an it, as a singular thing. It's suggesting we call the Internet one thing and the rest of the world some other thing. There are a lot businesses in the world I wouldn't do business with. When a guy in New York on a street corner offers me a Rolex for $20 I don't do business with him, and when he asks me questions on the Internet, tell me your health information on the Internet, I don't give him that either. And I think to try to create laws to respond to that sort of corner of commerce while we see the rest of it developing in a different way, in a way that I think the FTC is pushing the Department of Commerce to pursue——

Mr. DELAHUNT. Maybe it's the accessibility of it though. I mean there is something different. This is not walking into a store with having had a history for most of us. This is something that really is so new that we do view it differently.

Mr. Rotenberg and Ms. Mulligan.

Mr. ROTENBERG. If I may say, Mr. Delahunt, I agree with what you say and I think it is the sense that many of us today have about the Internet, but it's not the first time that people in this country have had that sense about a new technology. People had a very similar sense when the telephone first became available, and suddenly we had the ability to communicate instantly with family members and friends and business people all around the world. That was a radically new understanding of time and space and what technology made possible.

And it was interesting also that shortly after the development of the telephone Graham Bell developed techniques to encode the information so the technical means would be available, and Congress passed laws to protect the privacy of the communication. So it's new in one sense, but in another sense it's very familiar.

Mr. DELAHUNT. And there was a Congressional response.

Mr. ROTENBERG. Yes.

Mr. DELAHUNT. Ms. Mulligan.

Ms. MULLIGAN. To build upon that, Professor Cate said that as the technology is evolving we don't know what people's reasonable expectations of privacy are, and I think that's the wrong way to think about it. I think that our job is to make sure that people's expectations of privacy, which I would say are a fairly constant thing and I don't think they change necessarily, that we have to make sure that new environments don't expose people to unreasonable risks. I think that is the job of both the Administration, self-regulation and this Congress.

Mr. CATE. If I may just respond to that briefly, sir.

Mr. DELAHUNT. Professor.

Mr. CATE. To a certain extent that doesn't make any sense in the current environment because we currently go into businesses and provide data which, as we've all testified, is freely bought and sold. So the expectation, if it does not change, should be when you act on the Internet that data is freely available as well. So if we're not

going to inquire into what the specific expectation is, we would have to assume that the expectation is that the open market for information, which has supported markets and vigorous press and other institutions, is also going to apply on the Internet.

Ms. MULLIGAN. I think that might be a shared expectation of people like me and Marc who know what happens.

Mr. DELAHUNT. That is exactly the point.

Ms. MULLIGAN. When I was sitting around the living room last night with my neighbors and housemates they had no expectation that Kenneth Starr would be able to walk in off the street and get access to records of the books that they purchased, and that was not a welcomed realization for them.

Mr. DELAHUNT. I would just say, Professor, I think Ms. Mulligan has really struck a chord with me because I think most of us, and I dare say even the chairman, we don't deal every day in the Internet. There is a generational issue here too. So we're talking about understanding, if you will. I mean there is a cultural transformation going on here as well in terms of expectations that I think maybe a discrete segment of our society is able to understand and comprehend, but the vast majority of consumers, the patient who walks into the doctor's office, really doesn't have a clue, and I dare say a lot of doctors don't have a clue. Just one man's opinion.

Mr. COBLE. Well the gentleman from Massachusetts said it's a generational problem, and that even the chairman may be involved. Mr. Delahunt.

Folks, I want to thank both panels for their testimony, I want to thank the members of the subcommittee for their input, and the very attentive audience for your patience during this hearing. It has been a good hearing and it has directed attention to an area that is in dire need of attention.

Now, folks, it's not likely that Congress will do anything in a tangible way this session. We may never do anything in a tangible way but, on the other hand, circumstances may dictate that and require it.

This concludes the oversight hearing on the privacy in electronic communications. The record will remain open for 1 week. So if additional information is forthcoming, and if you have another night as you had last night, Ms. Mulligan and something comes to you, within the next week feel free to submit it.

Thank you all for your attendance.

The subcommittee stands adjourned.

[The subcommittee adjourned at 12:10 p.m., subject to the call of the Chair.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

ONE HUNDRED FIFTH CONGRESS
CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY

MEMORANDUM

TO: Members of the Subcommittee on Courts and Intellectual Propery

FROM: Howard Coble, Chairman

Barney Frank, Ranking Member

RE: Oversight hearing on privacy in electronic communications

DATE: March 26, 1998

On Thursday, March 26, at 10:00 am in Room 2237 RHOB, the Subcommittee will conduct an oversight hearing on privacy in electronic communications. In particular, the testimony will center around privacy over the Internet, privacy in electronic telecommunications, and whether and to what extent changes in the law or government regulation is necessary.

Enclosed please find two CRS reports (97–833A, 92–959A). They both contain a comprehensive discussion on the issues that will be the subject of the hearing.

PREPARED STATEMENT OF HOWARD COBLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA, AND CHAIRMAN, SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

Today, the Subcommittee will conduct an oversight hearing on privacy in electronic communications. This hearing was suggested by the Ranking Member of this Subcommittee, Mr. Frank, and I am pleased to begin exploring this very important issue. In the technologically advanced world in which we live, privacy in electronic communications is of vital importance to individuals and businesses. The ability to intercept, descramble and eavesdrop on private electronic communication over the Internet and cellular and digital communications places the privacy of individuals and businesses in jeopardy. That it turn, deteriorates the incentive for individuals and businesses to engage in electronic commerce, and as a result stifles the growth of American business. It also places the fundamental right of individuals to keep personal information private at risk.

I look forward to an informative and educational hearing.

92-959 A

CRS Report for Congress

Wiretapping & Electronic Surveillance: The Electronic Communications Privacy Act and Related Matters

Charles Doyle
Senior Specialist
American Public Law

December 10, 1992

Congressional Research Service • The Library of Congress

WIRETAPPING & ELECTRONIC SURVEILLANCE; THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND RELATED MATTERS

SUMMARY

At a time when individual privacy is fast becoming an illusion, electronic meddlers and eavesdroppers bent on industrial or political eavesdropping seem to have become more prevalent. The Electronic Communications Privacy Act (ECPA) and its equivalents at state law outlaw such misconduct.

Subject to a few exceptions, it is a federal crime to use a device to intentionally:

- secretly eavesdrop upon or record the telephone conversations of others;
- secretly eavesdrop upon or record the private face-to-face conversations of others;
- use information that is the fruit of criminal eavesdropping;
- disclose information that is the fruit of criminal eavesdropping;
- possess equipment primarily designed to secretly capture conversation;
- capture a telephone conversation involving a cordless phone;
- use a scanner to capture cellular phone conversations (but the penalties may be minor if the use is relatively innocent);
- intercept nonverbal communications such as telex;
- secretly gain access to the e-mail messages of others;
- gain unauthorized access to computer stored communications; or
- secure the telephone numbers called from a particular phone or called into a particular phone.

Although the conduct may be prosecuted as a state crime in some jurisdictions, it is generally *not* a federal crime to use a device to:

- record your own telephone conversation or to hear or record someone-else's telephone conversation with the permission of one of the parties;
- "monitor" someone else's telephone conversation over a regular extension phone for business purposes;
- record your own face-to-face conversations or to hear or record someone else's conversation with the permission of one of the parties;
- hear or record any public conversation or other discussion occurring under circumstances where the speakers should reasonably have anticipated that they would have been overheard;
- use everyday radio equipment to capture conversations or other radio communications;
- use or disclose the fruits of lawful eavesdropping.

The telephone company and others who provide communication service, and the police and government intelligence agents acting under court supervision, enjoy greater latitude to intercept communications.

TABLE OF CONTENTS

WIRETAPPING AND ELECTRONIC SURVEILLANCE: THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND RELATED MATTERS

INTRODUCTION

At a time when individual privacy is fast becoming an illusion, electronic meddlers and eavesdroppers bent on industrial or political espionage seem to have become particularly prevalent. The Electronic Communications Privacy Act (ECPA) and its equivalents at state law outlaw such misconduct. This is a quick look at their provisions with a primary focus upon intrusions other than those conducted for law enforcement purposes.[1]

ECPA and its state counterparts outlaw wiretapping, electronic eavesdropping, and other forms of using a machine or device to secretly capture the communications of others.[2] They also condemn the use or disclosure of the fruits of wiretapping or electronic eavesdropping[3] and even the possesson of

---

[1] For a more extensive examination of wiretapping and electronic surveillance as law enforcement tools, see Carr, The Law of Electronic Surveillance (1989), and Fishman, Wiretapping and Eavesdropping (1989).

Since its focus is not the protection afforded the commercial exploitation of words or ideas, this report skirts the related mysteries of the copyright law, patent law, and trade secrets; for a discussion of those areas see, Nimmer, Nimmer on Copyright (1992); Lipscomb, Walker on Patents (1989); Chisum, Patents; Jager, Trade Secrets Law (1992); Milgrim, Milgrim on Trade Secrets (1990).

[2] Here and elsewhere the forms of eavesdropping are divided into three types of interceptions: wire, oral and electronic; that is, eavesdropping accomplished by wiretapping or intercepting wire communications; that accomplished by secretly listening in on face-to-face conversations or intercepting oral communications; and secretly capturing other forms of communications such as telex messages or electronic mail messages stored in a computer or intercepting electronic communications. For citations to state statutes outlawing interception, see Appendix A.

[3] For citations to state statutes see Appendix D.

interception equipment.[4] Offenders invite federal and state civil as well as criminal liability.[5]

Subject to a few exceptions, it is a federal crime to use a device to intentionally:

- secretly eavesdrop upon or record the telephone conversations of others;

- secretly eavesdrop upon or record the private face-to-face conversations of others;

- use information that is the fruit of criminal eavesdropping;

- disclose information that is the fruit of criminal eavesdropping;

- possess equipment primarily designed to secretly capture conversation;

- capture a telephone conversation involving a cordless phone;

- use a scanner to capture cellular phone conversations (but the penalties may be minor if the use is relatively innocent);

- intercept nonverbal communications such as telex;

- secretly gain access to the e-mail messages of others;

- gain unauthorized access to computer stored communications; or

- secure the telephone numbers called from a particular phone or called into a particular phone.

Although the conduct may be prosecuted as a state crime in some jurisdictions, it is generally *not* a federal crime to use a device to:

- record your own telephone conversation or to hear or record someone else's telephone conversation with the permission of one of the parties;

- "monitor" someone else's telephone conversation over a regular extension phone for business purposes;

---

[4] For citations to state statutes see Appendix E.

[5] Attorneys who wiretap or eavesdrop may be acting contrary to the ethical standards of their profession, see *Undisclosed Recording of Conversations by Private Attorneys*, 42 South Carolina Law Review 995 (1991) and the cases and bar association advisory opinions which it cites.
For citations to state civil liability statutes see Appendix F.

- record your own face-to-face conversations or to hear or record someone else's conversation with the permission of one of the parties;

- hear or record any public conversation or other discussions occurring under circumstances where the speakers should reasonably have anticipated that they would have been overheard;

- use everyday radio equipment to capture conversations or other radio communications;

- use or disclose the fruits of lawful eavesdropping.

The telephone company and others who provide communication service, and the police and government intelligence agents acting under court supervision, enjoy greater latitude to intercept communications.

BACKGROUND

At common law, "eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior."[6]

Although early American law proscribed common law eavesdropping as well, it was little prosecuted and by the late nineteenth century had "nearly faded from the legal horizon."[7] Instead, state wiretap laws and statutes outlawing indiscretion by telephone and telegraph operators preserved the spirit of the common law prohibition in this country.

By the time of the landmark Supreme Court decision in *Olmstead* in 1928, at least forty-one of the forty-eight states had passed laws forbidding telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or prohibiting wiretapping or both.[8] On the federal level,

---

[6] 4 Blackstone, Commentaries on the Laws of England, 169 (1769).

[7] "Eavesdropping is indictable at the common law, not only in England but in our states. It is seldom brought to the attention of the courts, and our books contain too few decisions upon it to enable an author to define it with confidence. . . . It never occupied much space in the law, and it has nearly faded from the legal horizon." 1 Bishop, Commentaries on the Criminal Law, 670 (1882).

[8] *Olmstead* v. *United States*, 277 U.S. 438, 479-80 n.13 (1928)(Brandeis, J., dissenting). *Olmstead* is remembered most today for the dissents of Holmes and Brandeis, but for four decades it stood for the view that the Fourth Amendment's search and seizure commands did not apply to government

Congress had enacted a wiretap statute,[9] but it was only designed to protect government secrets during World War I[10] and remained in effect only until the end of the War. It was not until the Federal Communications Act of 1934 that Congress passed general legislation to protect the privacy of telegraph and telephone conversations.[11]

Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[12] when it had become apparent that technology had outstripped the protection of the Communications Act and after the Supreme Court repudiation of *Olmstead* necessitated a procedural scheme for electronic surveillance for law enforcement purposes.[13]

Title III was subsequently supplemented with the Foreign Intelligence Surveillance Act,[14] which afforded more specific authorization and more specific protection in the area of national security intelligence gathering.

Most recently, Congress again sought to bring the law abreast of surveillance technology with the Electronic Communications Privacy Act of 1986 (ECPA). The Act followed the general outline of Title III with adjustments and additions. Like Title III, it sought to strike a balance between the interests of privacy and law enforcement, but it also reflected a Congressional desire to avoid unnecessarily crippling infant industries in advanced communications technology.[15]

---

wiretapping accomplished without a trespass onto private property.

[9] 40 Stat.1017 (1918).

[10] 56 Cong.Rec. 10761-765 (1918).

[11] 48 Stat. 1064, 1103-104 ("No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof . . . and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication. . . ." 47 U.S.C. 605 (1940 ed.)).
The Communications Act amended the Radio Act of 1927, 44 Stat. 1162, 1172 (1927), which as enacted contained the radio portion of this section.

[12] 87 Stat. 197, 18 U.S.C. 2510 - 2520 (1970 ed.).

[13] *Berger* v. *New York*, 388 U.S. 41 (1967); *Katz* v. *United States*, 389 U.S. 347 (1967).

[14] 92 Stat. 1783, 50 U.S.C. 1801 - 1811.

[15] H.R.Rep.No. 647, 99th Cong., 2d Sess. 18-9 (1984); S.Rep.No. 541, 99th Cong., 2d Sess. 5 (1986).

INTERCEPTION

ECPA, in its revision of Title III, outlaws electronic surveillance, possession of electronic surveillance equipment, disclosure of information obtained through illegal electronic surveillance, and use of information secured through illegal electronic surveillance.[16] In separate chapters it regulates stored wire and electronic communications and transactional records access,[17] and pen registers and trap and trace devices.[18]

At ECPA's heart lies the prohibition against (1) intentionally, (2) intercepting, (3) wire, oral or electronic communications, (4) by using a mechanical device, (5) without permission or some other form of exception such as that provided for (6) some kinds of radio broadcasts, (7) the police, (8) the telephone company and others who help provide communications services, and (9) in some places, spousal wiretappers.[19]

---

[16] 18 U.S.C. 2511. For citations to state statutes see Appendices A., D. and E.

[17] 18 U.S.C. 2701 - 2711. For the citation to state statutes see Appendix B.

[18] 18 U.S.C. 3121 - 3127. For the citations to state statutes see Appendix C.

[19] "(1) Except as otherwise specifically provided in this chapter any person* who -- (a) intentionally intercepts,** endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communications***;

(b) intentionally uses, or endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device*^ to intercept any oral communication when --

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communicatlon; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has rsason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States. . . .

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)." 18 U.S.C. 2511(1)(a),(b)

ECPA contains two versions of the basic prohibition because Congress was

---

* "'person' means any employee, or agent of the United States, or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation," 18 U.S.C. 2510(6).

** "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," 18 U.S.C. 2510(4).

*** "'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications for communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such exception, but such term does not include any electronic communication;

'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include --

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(1),(2),(12).

*^ "'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than --

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigator or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal," 18 U.S.C. 2510(7).

uncertain of the bounds of its constitutional authority to enact a simple generic proscription.[20] The Justice Department has honored that caution by employing subparagraph (a) to prosecute wiretapping, while using subparagraph (b) to prosecute other forms of electronic surveillance.[21]

"INTENTIONALLY"

Conduct can only violate ECPA if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed.[22]

"INTERCEPT"

ECPA proscribes intentional interceptions. Interception "means the aural[23] or other acquisition of the contents" of various kinds of communications. ECPA enlarged the definition by adding the words "or other acquisition" to the definition so that it is no longer limited to interceptions that can be heard.

---

[20] "Subparagraph (a) establishes a blanket prohibition against the interception of wire communication. Since the facilities used to transmit wire communications form part of the interstate or foreign communications network, Congress has plenary power under the commerce clause to prohibit all interception of such communications whether by wiretapping or otherwise.

"The broad prohibition of subparagraph (a) is also applicable to the interception of oral communications. The interception of such communications, however, does not necessarily interfere with the interstate or foreign commerce network, and the extent of the constitutional power of Congress to prohibit such interception is less clear than in the case of interception of wire communications. . . .

"Therefore, in addition to the broad prohibitions of subparagraph (a), the committee has included subparagraph (b), which relies on accepted jurisdictional bases under the commerce clause, and other provisions of the Constitution to prohibit the interception of oral communications." S.Rep.No.1097, 90th Cong., 2d Sess. 91-2 (1968).

[21] 9 Department of Justice Manual §9-60.221 (1989 Supp.).

[22] "In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under title III of the Omnibus Crime Control and Safe Streets Act of 1968 from 'willful' to 'intentional.' . . . This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act." S.Rep.No. 541, 99th Cong., 2d Sess. 23 (1986); H.R.Rep.No. 647, 99th Cong., 2d Sess. 48-9(1986).

[23] The dictionary definition of "aural" is of or relating to the ear or to the sense of hearing.

"WIRE, ORAL OR ELECTRONIC COMMUNICATIONS"

An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects. Congress used the definitions of the three forms of communications to describe the communications beyond the Act's reach as well as those within its grasp. For example, the definition of "wire communications" expressly excludes that portion of a cordless phone conversation which could be easily and inadvertently captured by an everyday radio.[24] The definition has been expanded, however, to embrace telephone conversations involving a private telephone system, systems once beyond the reach of Title III.[25]

An "oral communication" includes one uttered under circumstances justifying an expectation of privacy but does not embody "electronic communications."[26]

---

[24] "'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications for communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but *such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit*," 18 U.S.C. 2510(1)(emphasis added).

"A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electric current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios." S.Rep.No. 541, 99th Cong., 2d Sess. 9 (1986).

[25] Prior to enactment of ECPA, federal law did not extent to wiretapping on private systems, see 18 U.S.C. 2510(1)(1982 ed.)(definition of "wire communications"); *United States* v. *Christman*, 375 F.Supp. 1354 (N.D.Cal. 1974). The definition was modified to specify "that wire, cable, or similar connections furnished or operated by any person engaged in providing or operating such facilities for the transmission of 'communications affecting interstate or foreign commerce,' are within the definition of a 'wire communication.' This language recognizes that private networks and intra-company communications systems are common today and brings them within the protection of the statute." S.Rep.No. 541, 99th Cong., 2d Sess. 11-2 (1986).

[26] "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such exception, but such term does

"Electronic communications" include other forms of information transfer but to the specific exclusion of certain radio transmissions which can be innocently captured without great difficulty.[27]

"DEVICE"

An interception can only be a violation of ECPA if an "electronic, mechanical, or other device" is used for the interception.[28] The definition of "device" specifically does not include a hearing aid and extension telephones under normal use.[29] Whether an extension phone has been installed and is being used in the ordinary course of business so that it no longer constitutes an interception device for purposes of ECPA and comparable state laws has proven

---

not include any electronic communication," 18 U.S.C. 2510(2).

[27] "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include –

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(12).

[28] "'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," 18 U.S.C. 2510(4).

Note that by inclusion of the phrase "or other acquisition," ECPA avoids the limitation of Title III which only reached interceptions which produced a result that could be heard by the human ear, S.Rep.No. 541, 99th Cong., 2d Sess. 13 (1986).

[29] "'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than –

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigator or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal," 18 U.S.C. 2510(7).

a somewhat vexing question.[30] Although often intertwined with the consent exception discussed below, the question generally turns on the facts in a given case.[31]

EXEMPTIONS: CONSENT INTERCEPTIONS

An interception is not a violation of ECPA if that Act declares the interception "not unlawful." There are four kinds of exemptions: consent exceptions, service provider exceptions, radio exceptions, and exceptions to reflect other federal regulations.

The ECPA left Title III's treatment of consent interceptions relatively unchanged.[32] There are two consent provisions, one for the police[33] and one

---

[30] See the cases cited and commentary in Barnett & Makar, "*In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 Hastings Journal of Communications and Entertainment Law 715 (1988); *Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§2510 et seq.), Pertaining to Interceptions of Wire Communications*, 58 ALR Fed. 594; *Eavesdropping on Extension Telephone as Invasion of Privacy*, 49 ALR 4th 430.

[31] See e.g., *Deal* v. *Spears*, 780 F.Supp. 618, 623 (W.D.Ark. 1991)(employer regularly taped employee calls by means of a device attached to an extension phone; most of the calls were personal and recording and disclosing them served no business purpose).

[32] The consent exemption arises from the view that the law ordinarily should not make it a crime to repeat conversations held with others and that someone who surreptitiously records or transmits a conversation is essentially no different from one who subsequently repeats it to others: "No different result is required if the agent of instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them . . . or [(2)] carries radio equipment which simultaneously transmits the conversations either to recording equipment . . . or to other agents. . . . If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's . . . justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks." *United States* v. *White*, 401 U.S. 745, 751 (1971).

[33] "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. 2511(2)(c).

for others.[34] Perhaps their most noteworthy feature is their limited application. They do no more than shield consent interceptions from the sanctions of Title III; they afford no protection from the sanctions of state law. Many of the states recognize a comparable exception, but some only permit interception with the consent of *all* parties to a communication.[35]

Under federal law, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument.[36] This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to protect.[37] Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.[38]

Private consent interceptions may not be conducted for a criminal or tortious purpose. At one time, the limitation encompassed interceptions for criminal, tortious, *or* otherwise injurious purposes, but ECPA dropped the reference to injurious purposes for fear that first amendment values might be threatened should the clause be read to outlaw consent interceptions conducted to embarrass.[39] The rule is still more easily stated than applied.[40]

---

[34] "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. 2511(2)(d).

[35] California, Delaware, Florida, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania and Washington are all party consent states, at least with respect to interception by private individuals. For citations to state law see Appendix G.

[36] *United States* v. *Horr*, 963 F.2d 1124 (8th Cir. 1992) (inmate use of prison phone); *Griggs-Ryan* v. *Smith*, 904 F.2d 112 (1st Cir. 1990)(use of landlady's phone).

[37] *Anthony* v. *United States*, 667 F.2d 870, 876 (10th Cir. 1981).

[38] *United States* v. *Antoon*, 933 F.2d 200, 203-204 (3d Cir. 1991).

[39] S.Rep.No. 541, 99th Cong., 2d Sess. 17-8 (1986); H.R.Rep.No. 647, 99th Cong., 2d Sess. 39-40 (1986).

RADIO COMMUNICATIONS

Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress signals, tone-only pagers, marine radio and citizen band radio transmissions, and transmissions from a cordless phone headset to the base unit. The exemption also embraces interceptions necessary to identify the source any transmission, radio or otherwise, disrupting communications satellite broadcasts.[41]

---

[40] "It is settled that the legality of an interception is determined by the purpose for which the interception is made, not by the subject of the communication intercepted. . . . Generally, when the purpose of an interception is to make or preserve an accurate record of a conversation in order to prevent future distortions by a participant, the interception is legal." *United States* v. *Underhill*, 813 F.2d 105, 110 (6th Cir. 1987), citing, *United States* v. *Truglio*, 731 F.2d 1123, 1131 (4th Cir. 1984); *By-Prod Corp.* v. *Armen-Berry Co.*, 668 F.2d 956, 959 (7th Cir. 1982); and *United States* v. *Phillips*, 564 F.2d 32, 33 (8th Cir. 1997). But *United States* v. *Vest*, 639 F.Supp. 899 (D.Mass. 1986), aff'd, 813 F.2d 477 (1st Cir. 1986), points out the difficulty of distinguishing between making a record of a criminal transaction "in order to prevent future distortions by a participant" and creating blackmail material.

[41] "It shall not be unlawful under this chapter or chapter 121 [relating to stored electronic communications and transaction action access records] of this title for any person --

(*i*) to intercept or access an electronic communications made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public";

(*ii*) to intercept any radio communication which is transmitted --

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any government, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio service; or

(IV) by any marine or aeronautical communications system;

(*iii*) to engage in any conduct which --

(I) is prohibited by section 633 of the Communications Act of 1934 [relating to unauthorized reception of cable service] or;

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act [relating to the unauthorized publication or use of wire or radio communications by those assisting it is transmission];

(*iv*) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source

LAW ENFORCEMENT

The police enjoy an exemption when acting under judicial authority, whether that provided in Title III for federal and state law enforcement officers,[42] the Foreign Intelligence Surveillance Act,[43] or the separate

---

of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in provision or the use of such system, if such communication is not scrambled or encrypted." 18 U.S.C. 2511(2)(g).

• "'[R]eadily accessible to the general public' means, with respect to a radio communication that such communication is not --

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25 [relating to satellite communications], subpart D, E, or F of part 74 [relating to remote pickup and auxiliary broadcasting], or part 94 of the Rules of the Federal Communications Commission [relating to private mixed microwave service], unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio," 18 U.S.C. 2510(16).

The cordless phone exemption is part of the definition of "wire communications," 18 U.S.C. 2510(1), supra n.19.

[42] "*Except as otherwise specifically provided in this chapter* any person who (a) intentionally intercepts . . . ." 18 U.S.C. 2511(1)(emphasis added).

[43] "(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." 18 U.S.C. 2511(2)(e).

provisions according them access to stored electronic communications and the use of pen registers and trap and trace devices.[44]

EXEMPTION FOR THE TELEPHONE COMPANY ET AL.

There is a general exemption for those associated with supplying communications services, the telephone company, switchboard operators, and the like. The exemption not only permits improved service and lets the telephone company protect itself against fraud,[45] but it allows for assistance to federal and state officials operating under a judicially supervised interception order.[46]

---

[44] "(h) It shall not be unlawful under this chapter --

(i) to use a pen register or a trap and trace device (as those terms are defined for the purpose of chapter 206). . . ." 18 U.S.C. 2511(2)(h).

For the citations to state statutes permitting judicial authorization of law enforcement interception of wire, oral or electronic communications, for access to stored electronic communications, and for the use pen registers and trap and trace devices see Appendix H.

[45] "(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks." 18 U.S.C. 2511(2)(a)(i).

"(h) It shall not be unlawful under this chapter --

* * *

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication service was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service." 18 U.S.C. 2511(2)(h)(ii).

[46] "(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian or other specified persons has been provided with --

(A) a court order directing such assistance signed by the authorizing judge, or

IMPLICIT EXEMPTION FOR SPOUSAL INTERCEPTION WITHIN THE HOME

Some of the federal courts of appeal have held that Title III does not preclude one spouse from wiretapping or electronically eavesdropping upon the other.[47] The exemption does not extend to interceptions by the agent of a spouse[48] and has been rejected by a majority of the circuits that considered the question.[49]

SANCTIONS

Interceptions in violation of Title III as amended by ECPA are generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[50] Victims are entitled to equitable relief; reasonable attorneys' fees and costs; damages in an amount equal to the greater of $10,000, $100 per day for each day of a violation, or the value of damage or gain attributable to the violation; and in appropriate cases, punitive damages, 18 U.S.C. 2520.

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. . . ." 18 U.S.C. 2511(2)(a)(ii).

[47] *Anonymous* v. *Anonymous*, 558 F.2d 677 (2d Cir. 1977); *Simpson* v. *Simpson*, 490 F.2d 803 (5th Cir. 1974).

[48] *Simpson* v. *Simpson*, 490 F.2d 803, 809 (5th Cir. 1974); *Nations* v. *Nations*, 670 F.Supp. 1432, 1434-436 (W.D.Ark. 1987).

[49] *Thompson* v. *Delaney*, 970 F.2d 744 (10th Cir. 1992); *Kempf* v. *Kempf*, 868 F.2d 970 (8th Cir. 1989); *Pritchard* v. *Pritchard*, 732 F.2d (4th Cir. 1984); *United States* v. *Jones*, 542 F.2d 661 (6th Cir. 1976).

[50] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title* or imprisoned not more than five years, or both." 18 U.S.C. 2511(4)(a).

* Section 3559 of title 18 classifies as a felony any offense punishable by imprisonment for more than one year; and as a class A misdemeanor any offense punishable by imprisonment for one year or less but not more than six months. Unless Congress clearly rejects the general fine ceilings it provides, section 3571 of title 18 sets the fines for felonies at not more than $250,000 for individuals and not more than $500,000 for organizations, and for class A misdemeanors at not more than $100,000 for individuals and not more than $200,000 for organizations. If there is monetary loss or gain associated with the offense, the offender may alternatively be fined not more than twice the amount of the loss or gain, 18 U.S.C. 3571.

Congress decided to mitigate punishment for two types of offenders. In order to minimize the opprobrium directed at radio scanner enthusiasts, use of a scanner or similar device to capture the radio portion of a message from a cellular phone, car phone or voice message pager is punishable by no more than a fine of not more than $500. Intentionally intercepting the non-radio portion of the same conversation is punishable by imprisonment for not more than a year and/or a fine of not more than $100,000. Subsequent offenses, interceptions committed for criminal or tortious purposes or motivated by commercial advantage or gain, and the capture of scrambled or encrypted conversations all carry the more stringent, basic penalty, imprisonment for not more than five years and/or a fine of not more than $250,000.[51]

Filching satellite communications is the second instance where Congress opted for reduced penalties. Unauthorized interception is broadly proscribed subject to an exception for unscrambled transmissions,[52] but interceptions for neither criminal, tortious, nor mercenary purposes, subject offenders to only civil liability.[53]

---

[51] "(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then –

(i) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than $500." 18 U.S.C. 2511(4)(b).

[52] "(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted –

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purpose of direct or indirect commercial advantage or private financial gain." 18 U.S.C. 2511(4)(c).

[53] "(5)(a)(i) If the communication is –

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial

VIDEO SURVEILLANCE

Concluding that video surveillance is the most intrusive form of surveillance, one federal appellate court panel held that Title III as amended by ECPA outlaws video surveillance.[54] The opinion was subsequently vacated in a decision which held that silent video surveillance is governed by the standards of the Fourth Amendment but not ECPA.[55]

STORED ELECTRONIC COMMUNICATIONS

Even in its modified form, Title III is ill suited to ensure the privacy of those varieties of modern communications which are equally vulnerable to intrusion when they are at rest as when they are in transmission. Surreptitious access is as least as great a threat as surreptitious interception to the patrons of electronic mail, electronic bulletin boards, and remote computer storage.

---

gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection --

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction." 18 U.S.C. 2511(5).

Under 18 U.S.C. 2520, victims may recover no more than damages of not less than $50 nor more than $500 for the first offense, increased to $100 and $1000 for subsequent offenses.

[54] *United States* v. *Koyomejian*, 946 F.2d 1450, 1458 (9th Cir. 1991), vacated, 970 F.2d 536 (9th Cir. 1992)(en banc).

[55] *United States* v. *Koyomejian*, 970 F.2d 536 (9th Cir. 1992)(en banc); see also, *United States* v. *Torres*, 751 F.2d 875 (7th Cir. 1984); *United States* v. *Biasucci*, 786 F.2d 504 (2d Cir. 1986); *United States* v. *Cuevas-Sanchez*, 821 F.2d 248 (10th Cir. 1990); *United States* v. *Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990).

Accordingly, while Title III governs interception, ECPA treats unlawful access to stored electronic communications beyond the confines of Title III. Unlawful access is a federal crime.[56] Violations committed for malicious or mercenary purposes are punishable by imprisonment for not more than a year and/or a fine of not more than $250,000; lesser transgressions, by imprisonment for not more than six months and/or a fine of not more than $5,000.[57] Those who provide the storage service and other victims of unlawful access have a cause of action for equitable relief, reasonable attorneys' fees and costs, damages equal the loss and gain associated with the offense but not less than $1000.[58]

---

[56] "Except as provided in subsection(c) of this section whoever –

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section." 18 U.S.C. 2701(a).

[57] "The punishment for an offense under subsection (a) of this section is –

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain –

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title [of not more than $250,00 for an individual and of not more than $500,000 for an organization with the alternative, if greater, of a fine equal to twice the gain or loss associated with the offense], or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case." 18 U.S.C. 2701(b).

[58] "(a) Cause of action. – Except as provided in section 2703(e)[relating to immunity for compliance with judicial process], any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) Relief. – In a civil action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection(c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred;

"(c) Damages. – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. . . ." 18 U.S.C.

The exceptions and exemptions mirror those of Title III. The proscriptions apply to "unauthorized" access; access authorized by the user or provider of the service is exempted.[59] There is a procedure for law enforcement and other government access notwithstanding the proscription, 18 U.S.C. 2702 - 2709, and exceptions for those who provide the communication service, 18 U.S.C. 2701(c)(1).

This seems to be the portion of ECPA least likely to have a clearly recognizable counterpart in state law. A few states have comparable legislation,[60] but in most jurisdictions the misconduct ECPA seeks to curtail is more likely the subject of statutes outlawing unauthorized computer access.[61]

PEN REGISTERS AND TRAP AND TRACE DEVICES

A trap and trace identifies the source of incoming calls, and a pen register indicates the numbers called from a particular phone. Since neither allows the eavesdropper to overhear the "contents" of the phone conversation they were not interceptions within the reach of Title III prior to the enactment of ECPA.[62] Although Congress elected to expand the definition of interception, it chose to continue to regulate these devices beyond the boundaries of Title III. Their use or installation by anyone other than the telephone company or those acting under judicial authority, however, is a federal crime.[63] Unlike other violations

---

2707.

[59] "(c) Exceptions. – Subsection (a) of this section does not apply with respect to conduct authorized –

(1) by the person or entity providing a wire or electronic communication service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703 [relating to government access], 2704 [relating to backup preservation at government insistence] or 2518 [relating to court interception authorizations issued under Title III] of this title." 18 U.S.C. 2701.

[60] See Appendix B.

[61] See appendix I.

Violation of ECPA's commands concerning stored electronic communications may also run afoul of the dictates of federal law concerning unlawful computer access, see 18 U.S.C. 1030.

[62] *United States* v. *New York Telephone Co.*, 434 U.S. 160 (1977).

[63] "(a) In general. – Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978. . . .

of ECPA, there is no separate federal cause of action for victims of a pen register or trap and trace device violation. Some of the states have established a separate criminal offense for unlawful use of a pen register or trap and trace device, yet most of these do seem to follow the federal lead and declined to establish a separate cause of action.[64]

CALLER ID

The telephone service commonly known as "Caller ID" is a display feature which identifies the telephone number of incoming calls. Is use or installation of Caller ID use or installation of a trap and trace device and therefore a federal crime?

Caller ID comes within the ECPA definition of a trap and trace device.[65] A telephone company which installs and a subscriber who uses the Caller ID feature have installed and used a trap and trace device.[66]

The statute supplies an exception for "a provider of electronic or wire communication service" for purposes of providing the service or preventing its abuse, for billing purposes and when acting with the consent of the service user. It supplies no exception for the service user. At least one federal court has

---

"(b) Exception. – The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service –

(1) relating to the operation, maintenance, and testing of a wire or communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

"(c) Penalty. – Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both." 18 U.S.C. 3121.

[64] See Appendix C.

[65] "As used in this chapter –

* * *

(4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted," 18 U.S.C. 3127(4).

[66] S.Rep.No. 247, 102d Cong., 1st Sess. 8 (1991).

refused to allow a telephone subscriber to claim a provider exception in the case of a violation of Title III.[67]

No federal court appears to have ruled upon the question directly. The two state supreme courts, called upon to consider whether Caller ID violated state trap and trace prohibitions, have reached opposite conclusions.[68]

A substantial number of state public utility commissions have approved requests to offer Caller ID services, although virtually all have required the telephone company to provide free call blocking which allows callers to prevent Caller ID display of their numbers.[69]

---

[67] *Rice* v. *Rice*, 951 F.2d 942 (8th Cir. 1991)(defense to civil liability under 18 U.S.C.2520(d)(3) for good faith reliance on 18 U.S.C. 2511(3)(telephone company exemption) is not available to an eavesdropping subscriber).

[68] *Southern Bell Tel. & Tel. Co.* v. *Hamm*, 409 S.E.2d 775 (S.C. 1991)(Caller ID does not violate South Carolina's trap and trace statute); *Barasch* v. *Bell Tel. Co.*, 605 A.2d 1198 (Pa. 1992)(Caller ID would violate the Pennsylvania trap and trace statute).

[69] *In re Southern Bell Tel. & Tel. Co.*, 123 PUR 4th 73 (Fla.Pub.Serv.Comm'n, 1991); *In re Southern Bell Tel. & Tel. Co.*, 123 PUR 4th 38 (N.C.Util.Comm'n, 1991); *In re Diamond State Tel. Co.*, 121 PUR 4th 317 (Del.Pub.Serv.Comm'n, 1991); *In re Chesapeake & Potomac Tel.Co.*, 118 PUR 4th 464 (Md.Pub.Serv.Comm'n, 1990); *In re US West Communications, Inc.*, 125 PUR 225 (Id.Pub.Util.Comm'n, 1991); *In re Central Tel.Co. of Ill.*, 126 PUR 4th 313 (Ill.Commerce Comm'n, 1991); *In re New England Tel. & Tel. Co.*, 127 PUR 4th 383 (Mass.Dept.Pub.Util., 1991); *In re New England Tel. & Tel. Co.*, 131 PUR 4th 341 (Vt.Pub.Serv.Bd., 1992); *In re US West Communications, Inc.*, 131 PUR 4th 486 (Ariz.Corp.Comm'n); *In re GTE South, Inc.*, 132 PUR 4th 553 (Ala.Pub.Serv.Comm'n, 1992); *In re Caller Identification Service*, 133 PUR 4th 79 (Wash.Util.Tel.Comm'n, 1992); *In re Call ID and Other Custom Local Area Signaling Services*, 133 PUR 4th 168 (Ore.Pub.Util.Comm'n, 1992); *In re US West Communications, Inc.*, 133 PUR 4th 326 (Colo.Pub.Util.Comm'n, 1992).

A few states have enacted statutes to the same effect, Cal.Pub.U.Code §2893; Me.Rev.Stat.Ann. tit.35-A, §§7101-A to 7105; Wis.Stat. §196.207. Presumably allowing callers to block the display of their numbers serves the same privacy interest as the trap and trace proscription.

The Federal Communications Commission issued a notice of proposed rule making on interstate caller identification service over a year ago, 56 Fed.Reg. 57300 (Nov. 8, 1991), but to date has not issued a rule.

DISCLOSURE AND USE OF INTERCEPTED INFORMATION

Title III, as amended by ECPA, prohibits the disclosure or use of information known to have been secured in violation of its proscriptions.[70] If interception is not unlawful under Title III, disclosure or use of the information is not unlawful under Title III. The same sentencing levels apply, and conduct which is not unlawful under Title III may nevertheless be criminal under state law or some other federal law.

While the prohibitions clearly apply beyond the wiretapper and eavesdropper, at some point the information presumably may become so publicly well known that further use or dissemination is no longer criminal. By the same token, the prohibitions probably do not taint knowledge from an independent source.[71]

ECPA does not ban disclosure or use of information acquired unlawfully from stored electronic communications or by means of a pen register or trap and trace device.[72] It does forbid the companies that provide the service from

---

[70] "(1) Except as otherwise specifically provided in this chapter any person who --

* * *

"(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

"(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

[71] See e.g., S.Rep.No. 1097, 90th Cong., 2d Sess. 93 (1968)("disclosure of the contents of an intercepted communication that had already become 'public information' or 'common knowledge' would not be prohibited").

[72] See 18 U.S.C. 2701 - 2710, 3121 - 3127, 2512.

disclosing the contents of stored communications[73] except for service or law enforcement purposes or with customer approval.[74]

Perhaps most surprising, ECPA grants express authority, without restriction, for the telephone company or any other communication service provider to disclose customer records to anyone other than the government.[75] It is not clear whether this grant of authority pre-empts state regulation.

---

[73] "(1) A person or entity providing an electronic communications service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote commuting service to the public shall not divulge to any person or entity the contents of any communication which is carried or maintained on that service --

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from) a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communication for purposes of providing any services other than storage or computer processing." 18 U.S.C. 2702(a).

[74] "A person or entity may divulge the contents of a communication --

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517 [relating to court approved interception of wire, oral or electronic communications], 2511(2)(a)[relating to service related interceptions of such communications], or 2703 [relating to government access to stored communications] of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of that service; or

(6) to a law enforcement agency, if such contents --

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime." 18 U.S.C. 2702(b).

[75] "(1)(A) Except as provided in subparagraph.(B)[relating to government access under warrant, subpoena or with customer consent], a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section [relating to the contents of communications in electronic storage or remote computer servicing]) to any person other than a governmental entity." 18 U.S.C. 2703(c)(1)(A).

POSSESSION OF EAVESDROPPING EQUIPMENT

Section 2512 outlaws the possession of equipment whose design "renders it primarily useful for . . . surreptitious interception,"[76] with exemptions for law enforcement and the telephone company.[77] Possession of equipment designed for lawful, but surreptitious use is unlawful,[78] although possession of equipment designed principally for lawful uses but clearly intended to be employed for criminal interception is lawful.[79] Possession of the spike mike

---

[76] "Except as otherwise provided in this chapter, any person who intentionally --

* * *

(b) manufactures, assembles, possesses, or sells any electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. . . shall be fined not more than $10,000 or imprisoned not more than five years, or both." 18 U.S.C. 2512(1)(b).

Section 2512 also outlaws mailing or advertising such devices, 18 U.S.C. 2512(1)(a),(c).

[77] "It shall not be unlawful under this section for --

(a) provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such provider, in the normal course of the business of providing that wire or electronic communications service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral or electronic communications." 18 U.S.C. 2512(2)(spacing at the end of subparagraph (b) supplied).

[78] *United States* v. *Bast*, 495 F.2d 138, 143-44 (D.C.Cir. 1974)("Thus, the manufacture, sale and possession prohibition was intended to ban particular devices, among them eavesdropping equipment which could be worn on the person of a party to a conversation, and hence used in a manner which would not violate §24511 because of its 'consent interception'").

[79] *United States* v. *Schweihs*, 569 F.2d 965, 968(5th Cir. 1978)("Thus, even though a device is constructed or purchased specifically for use in covert wiretapping or eavesdropping, as Schweihs' homemade operational amplifier may well have been, it is not proscribed by the statute if its design characteristics do not render it *primarily* useful that purpose")(emphasis in the

and the martini olive transmitter are unlawful; possession of the ordinary tape recorder concealed in the heating duct is not.[80] Several of the states supplement federal coverage by banning equipment designed or intended for unlawful rather than surreptitious use.[81]

The more contentious question, however, is whether section 2512 extends to possession of equipment designed to permit unauthorized reception of scrambled satellite television signals.[82]

---

original).

[80] Cf., *United States* v. *Pritchard*, 773 F.2d 873, 878-79 (7th Cir. 1985); *United States* v. *Pritchard*, 745 F.2d 1112, 1123-124(7th Cir. 1984); *United States* v. *Wynn*, 633 F.Supp. 595, 602 (C.D.Ill. 1986).

[81] See citations to state statutes in Appendix E.

[82] Compare, *United States* v. *McNutt*, 908 F.2d 561 (10th Cir. 1990); *United States* v. *Lande*, 968 F.2d 907 (9th Cir. 1992)(both holding that Title III forbids possession of descramblers to allow unauthorized viewing of scrambled satellite television programming), with *United States* v. *Herring*, 933 F.2d 932 (11th Cir. 1991); *United States* v. *Hux*, 940 F.2d 314 (8th Cir. 1991); *United States* v. *Shriver*, 782 F.Supp. 406 (C.D.Ill.L. 1992)(all holding that it does not); see also, *The Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 Minnesota Law Review 1451 (1992).

Appendix A.

State Statutes Outlawing the Interception of Wire(w), Oral(o) and Electronic Communications(e)[83]

Alabama: Ala.Code §13A-11-31(w/o);

Alaska: Alaska Stat. §42.20.300(w), 42.20.310(o);

Arizona: Ariz.Rev.Stat.Ann. §13-3005(w/o/e);

Arkansas: Ark.Code §23-17-107(w);

California: Cal.Penal Code §§631(w), 632(o);

Colorado: Colo.Rev.Stat. §§18-9-303(w), 18-9-304(o);

Connecticut: Conn.Gen.Stat.Ann. §§53a-188(w); 53a-189(o);

Delaware: Del.Code tit.11 §§1335(w) 1336(w/o);

Florida: Fla.Stat.Ann. §934.03(w/o/e);

Georgia: Ga.Code §16-11-62 (w/o);

Hawaii: Hawaii Rev.Stat. §803-42(w/o/e);

Idaho: Idaho Code §18-6702(w/o);

Illinois: Ill.Stat.Ann. ch.38 §14-2(w/o);

Iowa: Iowa Code Ann. §727.8(w/o);

Kansas: Kan.Stat.Ann. §21-4001(w/o); 21-4002(w);

Kentucky: Ky.Rev.Stat. §526.020(w/o);

Louisiana: La.Rev.Stat.Ann. §15:1303(w/o/e);

Maine: Me.Rev.Stat.Ann. ch.15 §§710(w/o);

Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402(w/o/e);

Massachusetts: Mass.Gen.Laws Ann. ch.272 §§99(w/o);

Michigan: Mich.Comp.Laws Ann. §§750.539c(o); 750.540(w);

Minnesota: Minn.Stat.Ann. §626A.02(w/o);

Montana: Mont.Code Ann. §45-8-213(w/o);

Nebraska: Neb.Rev.Stat. §86-702Ow/o);

Nevada: Nev.Rev.Stat. §§200.620(w), 200.650(o);

New Hampshire: N.H.Rev.Stat.Ann. §570-A:2(w/o);

New Jersey: N.J.Stat.Ann. §2A:156-3(w/o);

New Mexico: N.M.Stat.Ann. §30-12-1(w);

New York: N.Y.Penal Law §250.05(w/o/e);

North Carolina: N.C.Gen.Stat. §14-155(w);

North Dakota: N.D.Cent.Code §§12.1-15-02(w/o);

Ohio: Ohio Rev.Code §2953.52(w/o);

Oklahoma: Okla.Stat.Ann. tit.13 §176.3(w/o/e);

Oregon: Ore.Rev.Stat. §165.540(w/o/e);

Pennsylvania: Pa.Stat.Ann. tit.18 §5703(w/o/e);

Rhode Island: R.I.Gen.Laws §§11-35-21(w/o);

South Dakota: S.D.Cod.Laws §23A-35A-20(w/o);

Tennessee: Tenn.Code Ann. §§39-14-411(w), 65-21-110(w);

Texas: Tex.Penal Code. §16.02(w/o/e);

Utah: Utah Code Ann. §§77-23a-4J(w/o/e);

Virginia: Va.Code §19.2-62(w/o/e);

Washington: Wash.Rev.Code Ann. §9.73.030(w/o);

West Virginia: W.Va.Code §62-1D-3(w/o/e);

Wisconsin: Wis.Stat.Ann. §968.31(w/o/e);

Wyoming: Wyo.Stat. §7-3-602(w/o/e);

District of Columbia: D.C.Code §23-542(w/o).

---

[83] The designation "(e)" in this list merely indicates a proscription against the interception of electronic communications to codified proximate to similar bans on the interception of wire and/or oral communications. In the appendices which follow there are individual lists of the citations to state statutes concerning stored electronic communications and pen register and trap and trace devices.

Appendix B.

State Statutes Outlawing the Interception of Stored Electronic Communications

Arizona: Ariz.Rev.Stat.Ann. §13-3006;
Hawaii: Hawaii Rev.Stat. §803-47.5;

Minnesota: Minn.Stat.Ann. §626A.27;
Texas: Tex.Penal Code. §16.04;

Florida: Fla.Stat.Ann. §934.21;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-4A-02;
Pennsylvania: Pa.Stat.Ann. tit.18 §5714;
Utah: Utah Code Ann. §§77-23b-2.

Appendix C.

State Statutes Outlawing Pen Registers and Trap and Trace Devices

Arizona: Ariz.Rev.Stat.Ann. §13-3005;
Hawaii: Hawaii Rev.Stat. §803-42;

Louisiana: La.Rev.Stat.Ann. §15:1313;

Minnesota: Minn.Stat.Ann. §626A.35;

New York: N.Y.Penal Law §250.30;
Oklahoma: Okla.Stat.Ann. tit.13 §177.2;
Pennsylvania: Pa.Stat.Ann. tit.18 §5771;
South Dakota: S.D.Cod.Laws §23A-35A-22;
Utah: Utah Code Ann. §§77-23a-13;
West Virginia: W.Va.Code §62-1D-10;

Florida: Fla.Stat.Ann. §934.31;
Idaho: Idaho Code §18-6720;

Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-4B-02;
New Hampshire: N.H.Rev.Stat.Ann. §570-B:2;
North Carolina: N.C.Gen.Stat. §15A-261;
Oregon: Ore.Rev.Stat. §165.659;
South Carolina: S.C.Code §17-29-20;
Texas: Tex.Penal Code. §16.03;
Virginia: Va.Code §19.2-70.1;
Wisconsin: Wis.Stat.Ann. §968.34.

Appendix D.

State Statutes Prohibiting The Disclosure of Unlawfully Intercepted Communications[84]

Alabama: Ala.Code §13A-11-35;
Colorado: Colo.Rev.stat. §§18-9-303, 18-9-304;
Florida: Fla.Stat.Ann. §934.03;
Idaho: Idaho Code §18-6702;
Kansas: Kan.Stat.Ann. §21-4002;
Maine: Me.Rev.Stat.Ann. ch.15 §§710;

Massachusetts: Mass.Gen.Laws Ann. ch.272 §§99;
Nebraska: Neb.Rev.Stat. §86-702;
New Hampshire: N.H.Rev.Stat.Ann. §570-A:2;

Alaska: Alaska Stat. §42.20.300, 42.20.310;
Delaware: Del.Code tit.11 §1336;

Hawaii: Hawaii Rev.Stat. §803-42;
Illinois: Ill.Stat.Ann. ch.38 §14-2;
Kentucky: Ky.Rev.Stat. §526.060;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402;
Minnesota: Minn.Stat.Ann. §626A.02;

Nevada: Nev.Rev.Stat. §200.630;
New Jersey: N.J.Stat.Ann. §2A:156-3;

---

[84] Does not include statutes which forbid disclosure of information secured pursuant to court approved interception or while assisting in transmission.

North Dakota: N.D.Cent.Code §§12.1-15-02;
Oklahoma: Okla.Stat.Ann. tit.13 §176.3;
Pennsylvania: Pa.Stat.Ann. tit.18 §5703;
Texas: Tex.Code of Crim.Pro. §16.02;
Virginia: Va.Code §19.2-62;
Wisconsin: Wis.Stat.Ann. §968.31;
Ohio: Ohio Rev.Code §2953.52;
Oregon: Ore.Rev.Stat. §165.540;
Rhode Island: R.I.Gen.Laws §§11-35-21;
Utah: Utah Code Ann. §§77-23a-4;
West Virginia: W.Va.Code §62-1D-3;
Wyoming: Wyo.Stat. §7-3-602;
District of Columbia: D.C.Code §23-542.

Appendix E.

State Statutes Outlawing The Possession of Interception Devices[85]

Alabama: Ala.Code §13A-11-34;
California: Cal. Penal Code §§ 635;
Connecticut:Conn.Gen.Stat.Ann.§§54-41a;
Florida: Fla.Stat.Ann. §934.04;
Hawaii: Hawaii Rev.Stat. §803-43*;
Kentucky: Ky.Rev.Stat. §526.040;
Maine: Me.Rev.Stat.Ann. ch.15 §710*;
Massachusetts: Mass.Gen.Laws Ann. ch.272 §§99(c)(5)*;
Minnesota: Minn.Stat.Ann. §626A.03*;
New Hampshire: N.H.Rev.Stat.Ann. §570-A:3*;
New York: N.Y.Penal Law §250.10;
Oklahoma: Okla.Stat.Ann. tit.13 §176.3;
Rhode Island: R.I.Gen.Laws §§11-35-24;
Utah: Utah Code Ann. §§77-23a-5*;
West Virginia: W.Va.Code §62-1D-4;
Arizona: Ariz.Rev.Stat.Ann. §§13-3008;
Colorado: Colo.Rev.Stat. §§18-9-302;
Delaware: Del.Code tit.11 §1336*;
Georgia: Ga. Code §16-11-63;
Idaho: Idaho Code §18-6703;
Louisiana: La.Rev.Stat.Ann. §15:1304*;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-403*;
Michigan: Mich.Comp.Laws Ann. §750.539f*;
Mississippi: Miss.Code §41-29-533;
New Jersey: N.J.Stat.Ann. §2A:156-5*;
North Dakota: N.D.Cent.Code §§12.1-15-03*;
Pennsylvania: Pa.Stat.Ann. tit.18 §5705*;
Texas: Tex. Penal Code §16.02;
Virginia: Va.Code §19.2-63*;
Wyoming: Wyo.Stat. §7-3-603;
District of Columbia: D.C.Code §23-543*.

Appendix F.

Civil Liability for Interceptions Under State Law[86]

---

[85] * Statutes which like federal law outlaw equipment primarily designed for surreptitious rather than unlawful use.

[86] Statutes creating a cause of action for violations concerning stored communications specifically are designated (s).

Even in the absence of a statute, state law may recognize a common law cause of action sounding in privacy, see Restatement (Second) of Torts, §652B; *Nader* v. *General Motors Corp.*, 25 N.Y.2d 560, 307 N.Y.S.2d 647, 255 N.E.2d 765 (1970); *Billing* v. *Atkinson*, 489 S.W. 858 (Tex. 1973).

California: Cal. Penal Code §§ 637.2;
Connecticut:Conn.Gen.Stat.Ann.§§54-41r;
Hawaii: Hawaii Rev.Stat. §803-48;
Illinois: Ill.Stat.Ann. ch.38 §14-6;
Maine: Me.Rev.Stat.Ann. ch.15 §§711;

Massachusetts: Mass.Gen.Laws Ann. ch.272 §§99;
Minnesota: Minn.Stat.Ann. §§626A.02, 626A.13;
New Hampshire: N.H.Rev.Stat.Ann. §570-A:11;
New Mexico: N.M.Stat.Ann. §§30-12-11;
Pennsylvania: Pa.Stat.Ann. tit.18 §§5725, 5747(a);
Utah: Utah Code Ann. §§77-23a-4; 77-23A-11, 77-23b-8(a);
Washington: Wash.Rev.Code Ann. §9.73.060;
Wisconsin: Wis.Stat.Ann. §968.31;

Colorado: Colo.Rev.Stat. §§18-9-309.5;
Florida: Fla.Stat.Ann. §§934.10, 934.27(a);
Idaho: Idaho Code §18-6709;
Louisiana: La.Rev.Stat.Ann. §15:1312;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-410, 10-4A-08(a);
Michigan: Mich.Comp.Laws Ann. §750.539h;
Nevada: Nev.Rev.Stat. §§200.690;

New Jersey: N.J.Stat.Ann. §§2A:156-24;

Ohio: Ohio Rev.Code §2953.65;
Texas: Tex.Civ.Pract. & Pro. §§123.001 - 123.004;
Virginia: Va.Code §19.2-69;

West Virginia: W.Va.Code §62-1D-12;

Wyoming: Wyo.Stat. §7-3-609;
District of Columbia: D.C.Code §23-554.

Appendix G.

Consent Interceptions Under State Law[87]

Alabama: Ala.Code §13A-11-30 (one party consent);
Arizona: Ariz.Rev.Stat.Ann. §§13-3005 (one party consent);

California: Cal. Penal Code §§ 631, 632 (all party consent required to intercept any communication in which any party might have an expectation of privacy, *O'Laskey* v. *Sortino*, 224 Cal.App.3d 241, 273 Cal.Rptr. 674 (1990));
Connecticut: Conn.Gen.Stat.Ann. §§53a-187 to 53a-189 (one party consent);
Florida: Fla.Stat.Ann. §934.03 (all party consent);

Hawaii: Hawaii Rev.Stat. §803-42 (one party consent);
Illinois: Illinois courts appear to permit one party consent in spite of Ill.Stat.Ann. ch.38 §14-2 which seems to require consent of all

Alaska: Alaska Stat. §42.20.300, 42.20.310 (one party consent);
Arkansas: Ark.Code §§23-17-107 (outlaws wiretapping without authority, presumably one party consent; no electronic eavesdropping statute);
Colorado: Colo.Rev.stat. §§18-9-303, 18-9-304 (one party consent);

Delaware: Del.Code tit.11 §§1335, 1336 (all party consent);
Georgia: Ga.Code §16-11-66; Georgia courts have upheld the validity of one party consent, *Kemp* v. *State*, 201 Ga.App. 629, 411 S.E.2d 880 (1991); *Thompson* v. *State*, 191 Ga.App. 906, 383 S.E.2d 339 (1989);
Idaho: Idaho Code §18-6702 (one party consent);
parties, see *People* v. *Jansen*, 203 Ill.App.3d 985, 561 N.E.2d 312 (1990);

---

[87] In each of the states unless there is a more demanding state law, ECPA's one party consent provisions are controlling; although not noted here some of the party consent states permit one party consent in law enforcement cases.

Indiana: Ind.Code Ann. §35-33.5-1-5 (one party consent);
Iowa: Iowa Code Ann. §727.8 (one party consent);

Kentucky: Ky.Rev.Stat. §526.010 (one party consent);
Maine: Me.Rev.Stat.Ann. ch.15 §709 (one party consent);
Massachusetts: Mass.Gen.Laws Ann. ch.272 §§99 (all parties must consent);
Minnesota: Minn.Stat.Ann. §626A.02 (one party consent);
Missouri: Missouri has no wiretap or electronic surveillance statutes, therefore only federal law with its one party consent applies;
Nebraska: Neb.Rev.Stat. §86-702 (one party consent);
New Hampshire: N.H.Rev.Stat.Ann. §570-A:2 (all party consent);
New Mexico: N.M.Stat.Ann. §§30-12-1 (one party consent);
North Carolina: N.C.Gen.Stat. §14-155 (outlaws wiretapping with no mention of consent interception);
Ohio: Ohio Rev.Code §2953.52 (one party consent);
Oregon: Ore.Rev.Stat. §165.540 (one party consent for wiretapping and all parties must consent for other forms of electronic eavesdropping);
Rhode Island: R.I.Gen.Laws §§11-35-21 (one party consent);

South Dakota: S.D.Comp.Laws §§23A-35A-20 (one party consent);

Texas: Tex.Penal Code §16.02 (one party consent);
Vermont: Vermont has no wiretapping or electronic eavesdropping statutes, therefore the federal one party consent provisions are the only law that applies there;
Washington: Wash.Rev.Code Ann. §9.73.030 (all parties must consent);
Wisconsin: Wis.Stat.Ann. §968.31 (one party consent);

Kansas: Kan.Stat.Ann. §§21-4001,21-4002 (all party consent for wiretapping; one party consent for other forms of electronic eavesdropping);
Louisiana: La.Rev.Stat.Ann. §15:1303 (one party consent);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402 (all party consent);
Michigan: Mich.Comp.Laws Ann. §750.539c (all party consent);
Mississippi: Miss.Code §41-29-531 (one party consent);
Montana: Mont.Conde Ann. §§45-8-213 (all parties must consent);

Nevada: Nev.Rev.Stat. §§200.620, 200.650 (one party consent);
New Jersey: N.J.Stat.Ann. §§2A:156-4 (one party consent);
New York: N.Y.Penal Law §250.00 (one party consent);
North Dakota: N.D.Cent.Code §§12.1-15-02 (one party consent);

Oklahoma: Okla.Stat.Ann. tit.13 §176.4 (one party consent);
Pennsylvania: Pa.Stat.Ann. tit.18 §5704 (all parties must consent);

South Carolina: South Carolina does not appear to have a wiretapping or electronic eavesdropping statute, therefore the federal one party consent law is the only law that applies there;
Tennessee: Tenn.Code Ann. §§65-21-110, 39-3-1324 forbid wiretapping; the courts have upheld the validity of a police interception with one party consent, *State* v. *Eldridge*, 759 S.W. 756 (Tenn.Crim.App. 1988); *State* v. *Buford*, 666 S.W.2d 473 (Tenn.Crim.App. 1983);
Utah: Utah Code Ann. §§77-23a-4 (one party consent);
Virginia: Va.Code §19.2-62 (one party consent);

West Virginia: W.Va.Code §62-1D-3 (one party consent);

Wyoming: Wyo.Stat. §7-3-602 (one party consent);
District of Columbia: D.C.Code §23-542 (one party consent).

Appendix H.

Court Authorized Interception Under State Law[86]

Arizona: Ariz.Rev.Stat.Ann. §§13-3010, 13-3017(p/t), 13-3016(s);
Colorado: Colo.Rev.Stat. §§16-15-101 to 16-15-104;
Delaware: Del.Code tit.11 §1336

Georgia: Ga.Code §§16-11-64;

Idaho: Idaho Code §§18-6708 to 18-6708, 18-6721 to 18-6722(p/t);
Indiana: Ind.Code §§35-33.5-1-1 to 35-33.5-5-6;
Louisiana: La.Rev.Stat.Ann. §§15:1308 to 15:1311, 15:1314 to 15:1316; 73.1 to 14:73.5;

Massachusetts: Mass.Gen.Laws Ann. ch.272 §99;
Mississippi: Miss.Code §§41-29-501 to 41-29-535;
Nevada: Nev.Rev.Stat. §§179.410 to 179.515, 179.530(p/t);
New Jersey: N.J.Stat.Ann. §§2A:156A-8 to 2A:156A-23;
New York: N.Y.Crime.Pro. Law §§700.05 to 700.70, 705.00 to 705.35(p/t);
Ohio: Ohio Rev.Code §§2933.51 to 2933.64;

Oregon: Ore.Rev.Stat. §§133.721 to 133.739, 167. 657 to 167.673(p/t);
Rhode Island: R.I.Gen.Laws §§12-5.1-1 to 12-5.1-16, 12-5.2-1 to 12-5.2-5(p/t);
South Dakota: S.D.Cod.Laws §§23A-35A-1 to 23A-35A-19, 23A-35A-24 to 23A-35A-34;
Utah: Utah Code Ann. §§77-23a-8 to 77-23a-10, 77-23a-14(p/t), 77-23B-2 to 77-23B-9(s);
Washington: Wash.Rev.Code Ann. §§9.73.040 to 9.73.140;
Wisconsin: Wis.Stat.Ann. §§968.28 to 968.30, 968.35 to 968.37(p/t);

California: Cal.Penal Code §629 to 629.48;

Connecticut: Conn.Gen.Stat.Ann. §§54-41a to 54-41t;
Florida: Fla.Stat.Ann. §§934.06, 934.21 to 934.38(s), 934.32 to 934.34(p/t);

Hawaii: Hawaii Rev.Stat. §§803-41 to 803-47, 803-47.5 to 803-47.9(s);
Illinois: Ill.Stat.Ann. ch.38 ¶¶108A-1 to 108A-11, 108B-1 to 108B-14;
Kansas: Kan.Stat.Ann. §§22-1574 to 22-2576;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-406 to 10-409, 10-4A-01 to 10-4A-08(s), 10-4B-01 to 10-4B-05(p/t);
Minnesota: Minn.Stat.Ann. §§626A.05 to 626.12, 626A.24(s), 626A.35 to 626A.37(p/t);
Nebraska: Neb.Rev.Stat. §§86-703 to 86-712;
New Hampshire: N.H.Rev.Stat.Ann. §§570-A:1 to 570-A:10, 570-B:1 to 570-B:7(p/t);
New Mexico: N.M.Stat.Ann. §§30-12-1 to 30-12-10;
North Carolina: N.C.Gen.Stat. §§15-260 to 15-264(p/t);
Oklahoma: Okla.Stat.Ann. tit.13 §§176.7 to 176.14, 177.1 to 177.5(p/t);
Pennsylvania: Pa.Stat.Ann. tit.18 §§5708 to 5724, 5741 to 5749(s), 5771 to 5775(p/t);
South Carolina: S.C.Code §§17-29-10 to 17-29-50(p/t);
Texas: Tex.Crim.Pro. Code. §§18.20, 18.21 (s, p/t);
Virginia: Va.Code §§19.2-68, 19.2-70.2(p/t), 19.2-70.3(s);
West Virginia: W.Va.Code §62-1D-11;

Wyoming: Wyo.Stat. §§7-3-605, 7-3-607;
District of Columbia: D.C.Code §§23-546 to 23-556.

---

[86] Citations with no designation indicate the statutory provisions for court approved interception orders; those with a (p/t) designation indicate the statutory provisions for court authorized used of pen registers and trap and trace devices; and those with a (s) designation indicate the statutory provisions for government access to stored electronic communications.

Appendix I.

State Computer Crime Statutes

Alabama: Ala.Code §§13A-8-100 to 13A-8-103;
Arizona: Ariz.Rev.Stat.Ann. §13-2316;
California: Cal.Penal Code §502;

Connecticut: Conn.Gen.Stat.Ann. §§53a-250 to 53a-261;
Florida: Fla.Stat.Ann. §§815.01 to 815.07;
Hawaii: Hawaii Rev.Stat. §708-890 to 708-896;
Illinois: Ill.Stat.Ann. ch.38 ¶¶16D-1 to 16D-7;
Iowa: Iowa Code Ann. §§716A.1 to 716A.16;
Kentucky:Ky.Rev.Stat. §§434.840 to 434.860;
Maine: Me.Rev.Stat.Ann. ch.17-A §§431 to 433;
Massachusetts: Mass.Gen.Laws Ann. ch.266 §30;
Minnesota: Minn.Stat.Ann. §§609.87 to 609.891;
Missouri: Mo.Ann.Stat. §§569.093 to 569.099;
Nebraska: Neb.Rev.Stat. §§28-1341 to 28_1348;
New Hampshire: N.H.Rev.Stat.Ann. §638:16 to 638:19;
New Mexico: N.M.Stat.Ann. §§30-20-1 to 30-20-7;
North Carolina: N.C.Gen.Stat. §§14-453 to 14-457;
Ohio: Ohio Rev.Code §2913.81;

Oregon: Ore.Rev.Stat. §164.371;
Rhode Island: R.I.Gen.Laws §§11-52-1to 11-52-8;
South Dakota: S.D.Cod.Laws §§43-43B-1 to 43-43B-6;
Texas: Tex.Penal Code. §§33.01 to 33.03;

Virginia: Va.Code §§18.2-152.1 to 18.2-152.14;
West Virginia: W.Va.Code §§61-3C-1 to 61-3C-21;
Wyoming: Wyo.Stat. §§6-3-501 to 6-3-504.

Alaska: Alaska Stat. §§11.46.740, 11.46.985;

Arkansas: Ark.Code §§5-41-101 to 5-41-106;
Colorado: Colo.Rev.Stat. §§18-5.5-101, 18-5.5-102;
Delaware: Del.Code tit.11 §§931 to 937;

Georgia: Ga.Code §§16-9-92 to 16-9-94;
Idaho: Idaho Code §§18-2201, 18-2202;

Indiana: Ind.Code §§35-43-2-4 to 35-43-2-3;

Kansas: Kan.Stat.Ann. §21-3755;
Louisiana: La.Rev.Stat.Ann. §§14:73.1 to 14:73.5;
Maryland: Md.Code Ann. art. 27 §146;

Michigan: Mich.Comp.Laws Ann. §§752.791 to 752.797;
Mississippi: Miss.Code §§97-45-1 to 97-45-13;
Montana: Mont.Code Ann. §§45-6-310, 45-6-311;
Nevada: Nev.Rev.Stat. §§205.473 to 205.491;
New Jersey: N.J.Stat.Ann. §§2C:20-23 to 2C:20-33;
New York: N.Y.Penal Law §§156.00 to 156.50;
North Dakota: N.D.Cent.Code §12.1-06.1-08;
Oklahoma: Okla.Stat.Ann. tit.21 §§1951 to 1958;
Pennsylvania: Pa.Stat.Ann. tit.18 §3933;
South Carolina: S.C.Code §§16-16-10 to 16-16-20;
Tennessee: Tenn.Code Ann. §§39-14-601 to 39-14-603;
Utah: Utah Code Ann. §§76-6-702 to 76-6-705;
Washington: Wash.Rev.Code Ann. §§9A.52.110 to 9A.52.130;
Wisconsin: Wis.Stat.Ann. §943.70;

Selected Bibliography

Books & Articles

Abramovsky, *Surreptitious Recording of Witnesses in Criminal Cases: A Quest for Truth or a Violation of Law and Ethics?*, 57 Tulane Law Review 1 (1982)

Barnett & Makar, *"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 Hastings Journal of Communications and Entertainment Law 715 (1988)

Brownell, *The Public Security and Wire Tapping*, 39 Cornell Law Quarterly 154 (1954)

Carr, The Law of Electronic Surveillance (1989)

Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 University of Pennsylvania Law Review 793 (1989).

Donnelly, *Comments and Caveats on the Wiretapping Controversy*, 63 Yale Law Journal 799 (1954)

Fein, *Regulating the Interception and Disclosure of Wire, Radio, and Oral Communications: A Case Study of Federal Statutory Antiquation*, 22 Harvard Journal of Legislaiton 47 (1985)

Fishman, *Technologically Enhanced Visual Surveillance the Fourth Amendment: Sophistication, Availability and the Expectation of Privacy*, 26 American Criminal Law Review 315 (1989)

___, Wiretapping and Eavesdropping (1978) & (Dec. 1989 Supp.)

Goldsmith & Balmforth, *The Electronic Surveillance of Privileged Communications: A Conflict of Doctrines*, 64 South California Law Review 903 (1991)

Hernandez, *ECPA and Online Computer Privacy*, 41 Federal Communications Law Journal 17 (1988)

Kastenmeier, Leavy & Beier, *Communications Privacy: A Legislative Perspective*, 1989 Wisconsin Law Review 715

Masson, *The Foreign Intelligence Surveillance Act: Time for Reappraisal*, 24 International Lawyer 1043 (1990)

National Commission for the Study of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, Final Report (1976)

Rosenstein, *The Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 Minnesota Law Review 1451 (1992)

Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case in Opposition*, 118 University of Pennsylvania Law Review 169 (1969)

Turley, *The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court*, 79 Journal of Criminal Law & Criminology 66 (1988)

Notes & Comments

Addressing the New Hazards of the High Technology Workplace, 104 Harvard Law Review 1898 (1991)

Caller ID: Privacy Protector or Privacy Invader?, 1992 University of Illinois Law Review 219

Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment, 58 University of Chicago Law Review 1045 (1991)

Eavesdropping and Compromising Emanuations of Electronic Equipment: The Laws of England and the United States, 23 Case Western Reserve Journal of International Law 359 (1991)

The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Communication Technologies, 13 Rutgers Computer & Technology Law Journal 451 (1987)

The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis, 80 Georgetown Law Journal 843 (1992)

Terminally Nosy: Are Employers Free to Access our Electronic Mail? 96 Dickinson Law Review 545 (1992)

Undisclosed Recording of Conversations by Private Attorneys, 42 South Carolina Law Review 995 (1991)

Wiretapping and the Modern Marriage: Does Title III Provide a Federal Remedy for Victims of Interspousal Electronic Surveillance? 55 Dickinson Law Review 855 (1987)

ALR Notes

Applicability of Provisions of Omnibus Crime Control and Safe Streets Act of 1968 (18 USCS §2511(1)) to Interception by Spouse, or Spouse's Agent, of Conversations of Other Spouse in Marital Home, 55 ALR Fed. 936

Application of Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USCS §§2510 et seq.) Pertaining to Interceptions of Wire Communications, 58 ALR Fed. 594

Construction and Application of State Statutes Authorizing Civil Cause of Action by Person Whose Wire or Oral Communications Is Intercepted, Disclosed, or Used in Violation of Statutes, 33 ALR 4th 506

Eavesdropping on Extension Telephone as Invasion of Privacy, 49 ALR 4th 430

Interception of Telecommunications by or With Consent of Party as Exception Under 18 USCS §2511(2)(c) and (d), to Federal Proscription of Such Interceptions, 67 ALR Fed 429

Permissible Surveillance, Under State Communications Interception Statute, by Person Other than State or Local Law Enforcement Officer or One Acting in Concert with Officer, 24 ALR 4th 1208

Permissible Warrantless Surveillance, Under State Communications Interception Statute, by State or Local Law Enforcement Officer or One Acting in Concert with Officer, 27 ALR 4th 449

Propriety of Monitoring of Telephone Calls to or From Prison Inmates Under Title III of Omnibus Crime Control and Safe Streets Act (18 USCS §§2510 et seq.) Prohibiting Judicially Unauthorized Interception of Wire or Oral Communications, 61 ALR Fed. 825

State Regulation of Radio Paging Services, 44 ALR 4th 216

Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 USCS §§1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents, 86 ALR Fed. 782

97-833 A

CRS Report for Congress

Information Privacy

Gina Marie Stevens
Legislative Attorney
American Law Division

September 15, 1997

Congressional Research Service • The Library of Congress

INFORMATION PRIVACY

SUMMARY

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy and security of information. Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Threats to the privacy of information arise primarily as the result of the widespread increase in the availability and use of computers and computer networks. The Congress, the executive branch, courts, businesses, privacy advocates, Web sites, Internet service providers, and professional organizations confront many privacy issues.

As the cost of storing electronic information becomes less expensive, more information is stored and linked by use of the same key, such as the social security number. Data-mining software facilitates the use of electronic information for commercial, unauthorized, and unlawful purposes. Because of the power of computer networks to compile, analyze, share, and match electronic information, electronic information is potentially much more invasive. One result of these technological advances has been the rapid growth of the information industry. There are three participants in the information industry: government entities, direct marketers, and reference services. Consumer reporting agencies are also a source of personal information. Generally each participant gathers and distributes personally identifying information. The information may be gathered for one purpose, and sold for another.

Threats to the privacy of information also come from criminals and hackers. Hackers are reported to be gathering sensitive consumer information in order to commit financial fraud. Financial fraud is committed when there is enough information to deceive a creditor about the perpetrator's true identity. This practice is commonly referred to as **identity theft** -- the illegal use of personal identifying information -- to commit financial fraud.

Constitutional protection extends only to the protection of the individual against government intrusions and does not address many recurring threats to the privacy of information by private entities. Existing federal statutes do not comprehensively protect the informational privacy interests of individuals and businesses either. However, there are several federal laws that extend protection to certain types of information on a sector-by-sector basis.

Individuals and businesses concerned with privacy are looking to encryption, the use of algorithms and ciphers to scramble and descramble information, to keep information private. Encryption can also impede the ability of law enforcement and national security agencies to access electronic information. The federal government has a strong interest in preserving its ability to intercept and interpret electronic communications. Currently there are no limits on what strength of encryption can be used in the United States, but there are limits on the strength of encryption products that can be sold internationally. The Congress is currently examining several proposals regulating the availability of encryption products.

TABLE OF CONTENTS

Information Privacy

INTRODUCTION

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy and security of information.[1] Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Twenty years ago the Privacy Protection Study Commission recommended steps be taken to strike a proper balance between the individual's personal privacy interests and society's information needs.[2] This paper discusses some recent threats to the privacy of information.[3] These threats arise primarily as the result of the widespread increase in the availability and use of computers and computer networks, the corresponding increase in the amount and type of information created, the availability and use of information for unauthorized secondary purposes, and the lack of adequate computer security. Technological safeguards, such as encryption, are viewed as tools to enhance computer security and protect privacy. Encryption also has the potential to impede the ability of law enforcement and national security agencies to access electronic communications.[4] Congress is currently examining several legislative proposals concerning the availability of encryption products. The Congress,[5] the

---

[1] See, U.S. Govt. Information Infrastructure Task Force, *A Framework for Global Electronic Commerce* 10-12. Available: http://www.iitf.nist.gov/eleccomm/ecomm.htm (1997).

[2] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

[3] *"Are You For Sale?"* PC World Magazine, October 1996. Available: http://www.pcworld.com/workstyles/online/articles/oct96/1410forsale.html. *"Internet Opens Your Windows to Everyone: Invasion Sorely Tests Right to be Let Alone,"* N.Y. Times, Aug. 3, 1997, at 1A. *"Privacy on the Web,"* TIME Magazine, Aug. 19, 1997. Available: http://www.pathfinder.com. *"Privacy for Sale: Peddling Data on the Internet,"* The Nation, June 23, 1997, at 11. The complex issues related to the privacy of medical information are beyond the scope of this report.

[4] Denning and Baugh, *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism* (1997).

[5] For a list of privacy legislation introduced in the 105th Congress see, *EPIC (Electronic Privacy Information Center) Online Guide to 105th Congress Privacy and Cyber-liberties Bills.* Available: http://epic.org/privacy/bill_track.html. (July 10, 1997).

executive branch,[6] courts, businesses,[7] privacy advocates,[8] Web sites and Internet service providers,[9] and professional organizations[10] continue to confront many other issues associated with the security and privacy of information.

BACKGROUND

Privacy has become a "broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious physical surveillance, and mail interception. Individuals claim a right of privacy for an enormously wide range of issues from the right to practice contraception or have an abortion to the right to keep bank

---

[6] See, Federal Trade Commission, *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996). Available: http:www.ftc.gov/bcp/conline/pubs/privacy/privacy.htm. In June of 1997, the FTC held four days of hearings on technology tools and industry self-regulation regimes designed to enhance personal privacy on the Internet. Available: http://www.ftc.gov/bcp/privacy2/index.html. U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, *Options for Promoting Privacy on the National Information Infrastructure* (April 1997). Available: http://www.iitf.nist.gov/ipc/privacy.htm. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (March 1997).* Available: http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf. U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Sept. 1994) and *Issue Update on Information Security and Privacy in Network Environments* (June 1995). Social Security Administration, *Privacy and Customer Service in the Electronic Age* (September 1997). Available: http://www.ssa.gov.

[7] Privacy and American Business, *Handbook of Company Privacy Codes* Vol. 3 (1996).

[8] See, American Civil Liberties Union, *Take Back Your Data Campaign* (July 1997). Available: www.aclu.org/action/tbyd.html. Center for Democracy and Technology, *CDT Privacy Demonstration*. Available: http:www.cdt.org/privacy. Electronic Frontier Foundation, *Privacy Archive*. Available: http://www.eff.org/pub/Publications/CuD/Privacy. Electronic Privacy Information Center, *Surfers Beware: Personal Privacy and the Internet (June 1997). Available: http:www.epic.org/reports/surfer-beware.html.*

[9] Netscape Comm., *Netscape, Firefly and Verisign Propose Open Profiling Standard (OPS) to Enable Broad Personalization of Internet Services: More Than 60 Companies and Organizations Support Uniform Architecture that Protects Users' Privacy* (May 27, 1997). Available: http://search.netscape.com/newsref/pr/newsrelease411.html. World Wide Web Consortium (W3C), *Platform Privacy Preferences (P3) Project* (June 1997). Available: http://www.w3.org/P3/overview.html.

[10] Direct Marketing Association, *Guidelines for Personal Information Protection*. Available: http:www.the-dma.org; Interactive Services Association, *Protecting Your Privacy When You Go Online*. Available: http://www.isa.net/project-open/priv-broch.html.

records confidential."[11] Some advocate the expansion of this concept to include the right to "information privacy" for online transactions and personally identifiable information.[12] The term "information privacy" refers to an individual's claim to control the terms under which "personal information" – information that can be linked to an individual or distinct group of individuals (e.g., a household) – is acquired, disclosed, and used.[13] The right to privacy has also been characterized as the "the right to be let alone."[14] There is a perception among many that in our information driven society this right is under attack. The potential harm that can occur from unauthorized disclosures of such information has been well documented.[15]

Individuals and businesses increasingly rely upon computers and computer networks to transact business and to access the Internet. There are estimated to be over 9,400,000 host computers worldwide, of which approximately 60 percent are located within the United States, and are estimated to be linked to the Internet. This count does not include the personal computers people use to access the4 Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the Internet. This figure is expected to grow to 200 million Internet users by the year 1999.[16] Computers are used for many transactions today: electronic uniform product code (UPC) scanners, telephones, email, Caller ID, ATMs, credit cards, electronic tolls, video surveillance cameras, health insurance filings, catalog shopping, pharmacy records, and Internet access. The use of computers and computer networks for personal and business transactions has resulted in the creation of vast amounts of information. Information stored or transmitted via computers includes credit and financial information, health information, tax information, employment information, business information, trade secrets, proprietary information, and customer information.

Online users may voluntarily disclose personally identifying information, for example, to an online service provider for registration or subscription purposes, to a Web site, to a marketer of merchandise, in a chat room, on a

---

[11] See, David Flaherty, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill, 1989.

[12] See, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 Fed. Comm. L.J. 195 (1992).

[13] See, U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, Commentary ¶ 2 (1995). Available: http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html.

[14] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[15] See, J. Rothfeder, *Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret* 175-95 (1992).

[16] *ACLU v. Reno*, 117 S. Ct. 2329, 2334 (1997).

bulletin board, or to an email recipient.[17] Information about online users is also collected by Web sites through technology which tracks traces and portraits of every interaction with the network.[18]

When a person accesses a Web site, the site's server requests a unique ID from the person's browser (e.g., Netscape, Microsoft Internet Explorer). If the browser does not have an ID the server delivers one in a "cookie" file to the user's computer. This process is called "passing a cookie." Cookies are similar to the Caller ID feature on phone systems. Web sites can use cookies to track information about user behavior.[19] Web sites contend that the primary purpose for the use and collection of user data is so that the computer receiving the data can send the information file requested by a user to the user's computer, to permit Web site owners to understand activity levels at various areas within sites, and to build new Web applications tailored to individual customers. One widely criticized feature of "cookies" is that this activity is generally invisible to the user, and often occurs without user consent.

Information that is stored electronically often can be linked by use of the same key, such as the social security number. The widespread use of the social security number for secondary purposes (e.g., credit, financial, motor vehicle licensing, health insurance, etc.) has contributed to this phenomenon. A person's social security number, by itself, may have little value since it in and of itself does not convey information about a person's characteristics, interests, buying habits, etc. It may be useful though to a credit card company (to help verify an applicant's identity) and also to a direct marketer (to ensure that a solicitation is sent to the right person).

---

[17] A report by the National Telecommunications and Information Administration (NTIA) addressed the private sector collection, use, and dissemination of telecommunications-related personal information (TRPI) created in the course of an individual's subscription or use of a telecommunications service; and concluded that as the cost of digitally storing personal information becomes less expensive, the accumulation of personal information from disparate sources will become more cost-effective for users. U.S. Dept. of Commerce, *National Telecommunications and Information Administration, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995). Available: http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

[18] A recent survey of the current practices of 70 federal agency web sites regarding the use of personal information collected from online users found that 31 federal agencies collect personal identifying information primarily from guest books, comment forms, or feedback forms. It found that 11 of the 31 agencies that collect personally-identifiable information reportedly give notice of use on their sites. See, OMB Watch, "*A Delicate Balance: The Privacy and Access Practices of Federal Government World Wide Web Sites,*" (Aug. 1997). Available: http://ombwatch.org/ombw/info/balance.html.

[19] See, Vanderbilt University Owen Graduate School of Management, Commercialization of the World Wide Web: The Role of Cookies. Available: http://www2000.ogsm.vanderbilt.edu/cb3/mgt565a/group5/paper.group5.paper2.htm.

Technologies like data-mining software facilitate the use of this information for commercial, unauthorized, and unlawful purposes. Because of the power of computer networks to quickly and inexpensively compile, analyze, share, and match digitized information, electronic information is potentially much more invasive. Computers make information multi-functional as vast amounts of consumer information are collected, generated, sorted, and disseminated electronically, and perhaps then sold, with or without consent. A wealth of personal information about individuals can be harvested. How valuable the information is depends in part on how descriptive it is and how it can be used. One result of these technological advances has been the rapid growth and expansion of the information industry.

INFORMATION INDUSTRY

Basically, there are three participants in the information industry -- government entities (federal, state, local), direct marketers, and reference services.[20] Generally each of them gathers and distributes personally identifying information. The information may be gathered for one purpose, and sold for another.

Examples of public records held by **government entities** that contain personally identifying information such as name, address, and social security number are: driver's licenses', driving records, marriage and divorce records, motor vehicle title and registration, vital statistics, voter registration records, political contribution records, firearm permits, property tax records, land records, SEC filings, court and law enforcement records, postal service address records, boat and aircraft records, financial and ethics disclosures, occupational and recreational licenses. Government records are generally available to anyone, and often represent significant sources of revenue for government agencies.

To determine who should be solicited for a particular product, service, or fund raiser, **direct marketers** rely on lists designed to target individuals who are likely to respond to solicitations. The list may be obtained from consumer surveys, warranty or response cards, and customer purchase data. The lists may also be merged with other lists or with information from other sources, such as public records and magazine subscriptions. Frequently, they rent preexisting lists from list brokers who group information such as similar interests, characteristics, and purchasing habits. The cost of renting a list varies depending upon the number of addresses on the list and the amount of information given.

---

[20] The section is derived from the report of the Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (March 1997).* Available: http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf.

Reference services gather information from a variety of sources, compile it, and then make it commercially available.[21] Common users of reference services include law firms, private investigators, and law enforcement officials. There are generally no federal laws on who can access information through a reference service. The service may require users to subscribe. The price of the information depends on how detailed the information is, how quickly it can be provided, and how frequently the subscriber uses the service.

Consumer reporting agencies are a source of a great deal of information about the consumer's finances: employer, credit card and loan account numbers, amount of available credit, amount of outstanding debt, payment histories, and default, judgment and bankruptcy information.

FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) regulates the credit reporting industry, places certain responsibilities on users of consumer reports, limits the circumstances in which consumer reporting agencies may disclose consumer reports, and requires consumer reporting agencies to investigate and report information the consumer claims is inaccurate or incomplete.[22] Under the FCRA consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose. FCRA defines "consumer report" as:

> "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under § 1681b."[23]

There are three key elements. First, the information must be reported by a consumer reporting agency. Second, the information that is collected must be used, or must be expected to be used, or collected in whole or in part for the purpose of serving as a factor in determining the consumer's eligibility for consumer credit or insurance, employment, or for another permissible purpose.

---

[21] See, *The Lexis-Nexis P-TRAK Service*, Library of Congress, Congressional Research Service Rep. No. 96-795A by Gina Marie Stevens, Sep. 30, 1996.

[22] Extensive amendments were made to the FCRA in September 1996, which generally become effective September 30, 1997. Pub. L. No. 104-208, §§2401-2422, 110 Stat. 3009 (1996).

[23] 15 U.S.C. § 1681a(d)(1).

Third, the information must bear on at least one of the seven enumerated characteristics.[24]

A consumer report contains identifying information, credit information,[25] public record information,[26] and information on inquiries.[27] Identifying information in the consumer report includes the consumer's name (and any prior name), current and previous addresses, birth date and social security number. This identifying information about consumers is often called "header information" in reference to its placement at the "head" of the consumer report. Consumer reporting agencies sell credit header information because it is not considered a consumer report and is therefore not subject to the FCRA.[28]

The Federal Trade Commission's commentaries to the FCRA have been interpreted not to prohibit the disclosure of credit header information for purposes other than credit, insurance, employment, or any of the other permissible purposes. The Commentaries state that "a report limited solely to the consumer's name and address alone, with no connotations as to credit worthiness or other characteristic, does not constitute a 'consumer report,' if it does not bear on any of the seven factors."[29] Recently a federal district court held that information disclosed by a consumer reporting agency containing names, current and former addresses, and social security numbers is not a consumer report within the meaning of the FCRA because the information did not bear on plaintiffs' credit or general character, nor was it used to establish their eligibility for credit, employment or any of the other permissible purposes.[30]

---

[24] 16 C.F.R. Part 600, Ax. section 603(d).

[25] Credit information in the consumer report typically includes bank, retail, credit card, and other lender account information.

[26] Public record information includes records concerning bankruptcy, tax liens, and judgments.

[27] Inquiry information includes the names of parties who have recently obtained copies of the consumer report.

[28] Reference services often purchase header information which is then put into a searchable database. Often the reference service will also have merged information from public records with credit header information.

[29] 16 C.F.R. Part 600 Ax. section 603.

[30] *Dotzler v. Perot, Laughlin v. Perot*, 914 F. Supp. 328 (E.D. Mo. 1996); see also *Hoke v. Retail Credit Corp.*, 521 F.2d 1079, 1081 (4th Cir, 1975), cert. denied, 423 U.S. 1087 (1976).

FINANCIAL FRAUD

Threats to the privacy of digital information also come from criminals and hackers.[31] In 1995 a hacker was arrested and accused of stealing millions of dollars worth of files and more than 20,000 credit-card account numbers from the Internet.[32] A recent GAO report on Information Security concluded that unknown and unauthorized persons are increasingly attacking and gaining access to highly sensitive information in the Department of Defense's computer systems.[33]

Hackers are reported to be gathering sensitive consumer information in order to commit financial fraud. The information most commonly used to commit financial fraud includes the social security number, mother's maiden name, prior addresses, date of birth, employment information (including salary), and credit card, loan, and other financial account numbers. There is a great deal of concern about the availability of any one of these pieces of information because of the ease with which additional pieces of information can be obtained. A mother's maiden name may be considered valuable information in the credit granting process in order to verify a consumer's identity, but not considered sensitive in the context of genealogical research. Financial fraud is committed when there is enough information to deceive a creditor about the perpetrator's true identity.

This practice is commonly referred to as identity theft -- the illegal use of personal identifying information -- including name, address, social security numbers, and date of birth -- to commit financial fraud. One particular type of identity theft occurs when the criminal "takes over" a consumer's account by changing the consumer's address for an existing account or submitting a fraudulent credit application to open an account in the consumer's name, but giving a different address as the place to send the card. Financial fraud includes obtaining a credit card under an assumed name, using another person's credit or debit card without authorization, applying for and receiving a loan using an assumed identity, or making unauthorized withdrawals or transfers from another person's checking or deposit account.

The Report of the Board of Governors of the Federal Reserve Board (FRB) indicated that there is little available data on aggregate losses to insured depository institutions due to fraud. Gross fraud charge-offs for

---

[31] Lohr, Steve, *Feeling Insecure Are We? Go Ahead, Be Paranoid. Hackers Are Out to Get You*, New York Times, B1, Mar. 17, 1997.

[32] *Business Technology: Security is Lost in Cyberspace*, N.Y. Times, Feb. 22, 1995, § D, at 1, col. 3.

[33] U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense pose Increasing Risks:* Testimony before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate. (May 22, 1996) GAO/T-AIMD-96-92.

Mastercard/Visa in 1995 were $790 million. The FRB estimated that check fraud for commercial banks, savings institutions, and credit unions totalled $615 million in 1995. Losses due to identity theft are not tracked separately from other types of fraud. In the opinion of the FRB, fraud losses related to the use of sensitive information likely play a small role in overall fraud losses and pose no significant threat to insured depository institutions.

As criminals take advantage of the Internet, federal investigative authorities expect to make increased use of electronic on-line surveillance.[34]

THE PRESIDENT'S INFORMATION INFRASTRUCTURE TASK FORCE

A host of questions are raised by the proliferation of personal and business information. Does a firm have a right to sell information about its customers? With or without its customers knowledge or consent? Do consumers have a right to privacy in online environments? Should commercial web providers' ability to collect information about its customers be regulated? Can industry self-regulation work? Is the information available secure? How frequent are violations occurring? What the penalties are for those who abuse the system? What is the likelihood of detecting those who commit fraud or abuse?

The President's Information Infrastructure Task Force recommends a market-oriented non-regulatory strategy to promote global electronic commerce on the Internet, and supports industry developed standards for privacy protection based on the following principles: data-gatherers should inform consumers what information they are collecting, and how they intend to use such data; data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information; consumers also would be entitled to redress if they are harmed by improper use or disclosure of personal information, if it is based on inaccurate, outdated, incomplete, or irrelevant personal information; and special protections for children's data and sensitive data (medical) should exist. To ensure that disparate privacy policies around the world provide adequate privacy protection and do not impede the flow of data on the Internet, the United States plans to engage its major trading partners in discussions to build support for a market based approach to privacy, and to continue discussions with European Union nations to resolve any problems that could threaten data flows.[35]

---

[34] *See* Prepared Testimony of Charles L. Owens, Chief Financial Crimes Section Federal Bureau of Investigation Before Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, Mar. 19, 1997.

[35] *President's Adviser on Electronic Commerce to Raise U.S. Concerns Over EU Privacy Rule* 14 BNA Intl Trade Rptr 1479 (Sept. 3. 1997).

The European Union Directive on the Protection of Personal Data will become effective October 1998.[36] It comprises a general framework of data protection practices for the processing of personal data, which it defines as "any information relating to an identified or identifiable natural person." The Directive is extraordinarily comprehensive.[37] It will require each of the sixteen EU member states to enact laws governing the "processing of personal data." The Directive defines "processing" as "any operation or set of operations" whether automated or not, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." The Directive obligates EU Member States to prohibit data transfers to non-European countries that do not have "adequate levels of protection" for personal data. The European Commission has recently released a paper expressing concern that the data protection practices of the United States (self-regulatory codes of conduct) will not be deemed "adequate protection" under the Directive.[38]

PRIVACY LAW

Informational privacy is protected by the Constitution in a limited number of ways. However, constitutional protection extends only to the protection of the individual against government intrusions and does not extend to many of the information privacy threats addressed in this paper. The Fourth Amendment search-and-seizure provision protects a right of privacy by requiring warrants before government may invade one's internal space or by requiring that warrantless invasions be reasonable. A "'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[39] However, "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all."[40] Similarly, the Fifth Amendment's self-incrimination clause was once thought of as a source of protection from governmental compulsion to reveal one's private papers,[41] but

---

[36] *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Eur. O.J. L281/31 (Nov. 23, 1995).*

[37] See, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 Iowa L.J. 431-734 (1995).

[38] European Commission, *First Orientations on Transfers of Data to Third Countries -- Possible Ways Forward in Assessing Adequacy*, 14 BNA Intl. Trade Rptr. 1338 (July 30, 1997).

[39] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[40] *Katz v. United States*, 389 U.S. 347, 350 (1967).

[41] *Boyd v. United States*, 116 U.S. 616, 627-630 (1886).

the Court has refused to interpret the self-incrimination clause as a source of privacy protection.[42] First Amendment principles also bear on privacy, both in the sense of protecting it,[43] but more often in terms of overriding privacy protection in the interests of protecting speech and press.[44] Finally, the due process clause of the Fifth and Fourteenth Amendments, to some degree, may be construed to protect the "liberty" of persons in their privacy rights.[45]

A patchwork of federal statutory laws exists to protect the privacy of certain information. Existing federal statutes do not comprehensively protect the informational privacy interests of individuals and businesses. However, there are several federal laws that extend protection to certain types of information such as credit, cable, video, financial, and federal agency

---

[42] Fisher v. United States, 425 U.S. 391, 399 (1976).

[43] See, e.g., *Frisby v. Schultz*, 487 U.S. 474 (1988)(using privacy rationale in approving governmentally-imposed limits on picketing of home).

[44] See, e.g., *Florida Star v. B. J. F.*, 491 U.S. 524 (1989)(newspaper could not be liable for violating state privacy statute when it published the name of a rape victim that it had lawfully obtained through public sources).

[45] *Whalen v. Roe*, 429 U.S. 589 (1977).

information.[46] There is no comprehensive federal privacy statute, rather Congress has adopted a sector-by-sector approach.

ENCRYPTION

Increasingly individuals and businesses concerned with the privacy and security of information are looking to encryption, the use of highly sophisticated algorithms and ciphers to scramble and descramble information, to provide data security and protection from privacy intrusions and abuses of access to their data. A major purpose of encryption technology is to prevent crimes like industrial espionage and fraud. Although use of encryption products is likely to increase with increased use of personal computers, the need for privacy and security in business communications, referred to as "corporate privacy", is motivating the routine use of encryption software on a widespread global basis. Encryption is likely needed and can be used in any business that conducts commerce electronically.[47]

---

[46] Title III of the **Omnibus Crime Control and Safe Streets Act of 1968** addresses the interception of wire and oral communications. 18 U.S.C. §§ 2510-2521; **The Fair Credit Reporting Act of 1970** (FCRA) regulates the dissemination of consumer credit reports by consumer reporting agencies. 15 U.S.C. § 1681 (amended by Pub. L. No. 104-208); **The Privacy Act of 1974** places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. 5 U.S.C. § 552a.; **The Family Educational Rights and Privacy Act of 1974** governs access to student records. 20 U.S.C. § 1232g; **The Tax Reform Act of 1976** restricts the ability of the Internal Revenue Service to disclose individual tax return information. 26 U.S.C. § 6103; **The Right to Financial Privacy Act of 1978** restricts the ability of the federal government to obtain bank records from financial institutions. 12 U.S.C. § 3401; **Cable Communications Policy Act of 1984** limits the disclosure of cable television subscriber names, addresses, and utilization information for mail solicitation purposes. 47 U.S.C. § 551; **The Electronic Communications Privacy Act of 1986** (ECPA) amended the 1968 wiretap statute. It outlaws electronic surveillance, possession of electronic surveillance equipment, and use of information secured through electronic surveillance. The ECPA regulates stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, pen registers, and trap and trace devices. 18 U.S.C. §§ 2510-2522, 2701-2710, 2711; Video Privacy Protection Act of 1988 covers the disclosure of video rental records, 18 U.S.C. § 2710; **Driver's Privacy Protection Act of 1994** (effective October 1997) restricts disclosure of information contained in state motor vehicle records. 18 U.S.C. § 2721; **Health Insurance Portability and Accountability Act of 1996** (Pub. L. No. 104-191, codified at 42 U.S.C. 1320d note) mandates the establishment of uniform standards for the electronic transmission of financial and administrative health information, sets a deadline for congressional action on privacy legislation, and requires the Secretary of Health and Human Services to recommend privacy legislation by August 1997; **Telecommunications Act of 1996** (Pub. L. No. 104-104), section 702 limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers, and provides a right of access for individuals.

[47] See, *Encryption and Banking*, Library of Congress, Congressional Research Service, Rep. No. 97-835A by M. Maureen Murphy, Sep. 15, 1997.

Satisfying the security and privacy needs of businesses and individuals can result in the establishment of barriers to surveillance by government agents seeking to execute wiretap orders. The federal government has a strong interest in preserving its ability to intercept and interpret electronic communications for national security or law enforcement reasons.[48] As encryption technology becomes increasingly available, less expensive and easier to use, the government's access to electronic communications is constricted. The federal government has sought to control the use of encryption technology. Prior to the 1980's, control of the availability and use of cryptography was viewed as a national security issue focused on the U.S. maintaining a technological advantage over other countries and preventing encryption products from becoming available to criminals internationally.[49] Today the availability and use of cryptography has also become a domestic law enforcement issue. Thus, export controls and key recovery encryption are intended to preserve U.S. law enforcement and national security capabilities. Although there is no limit on what kind of encryption can be used in the United States, the government has imposed export controls, limiting the strength of the encryption products that can be sold internationally, on encryption products.[50] These export controls by extension may affect what type of encryption is available domestically.[51]

---

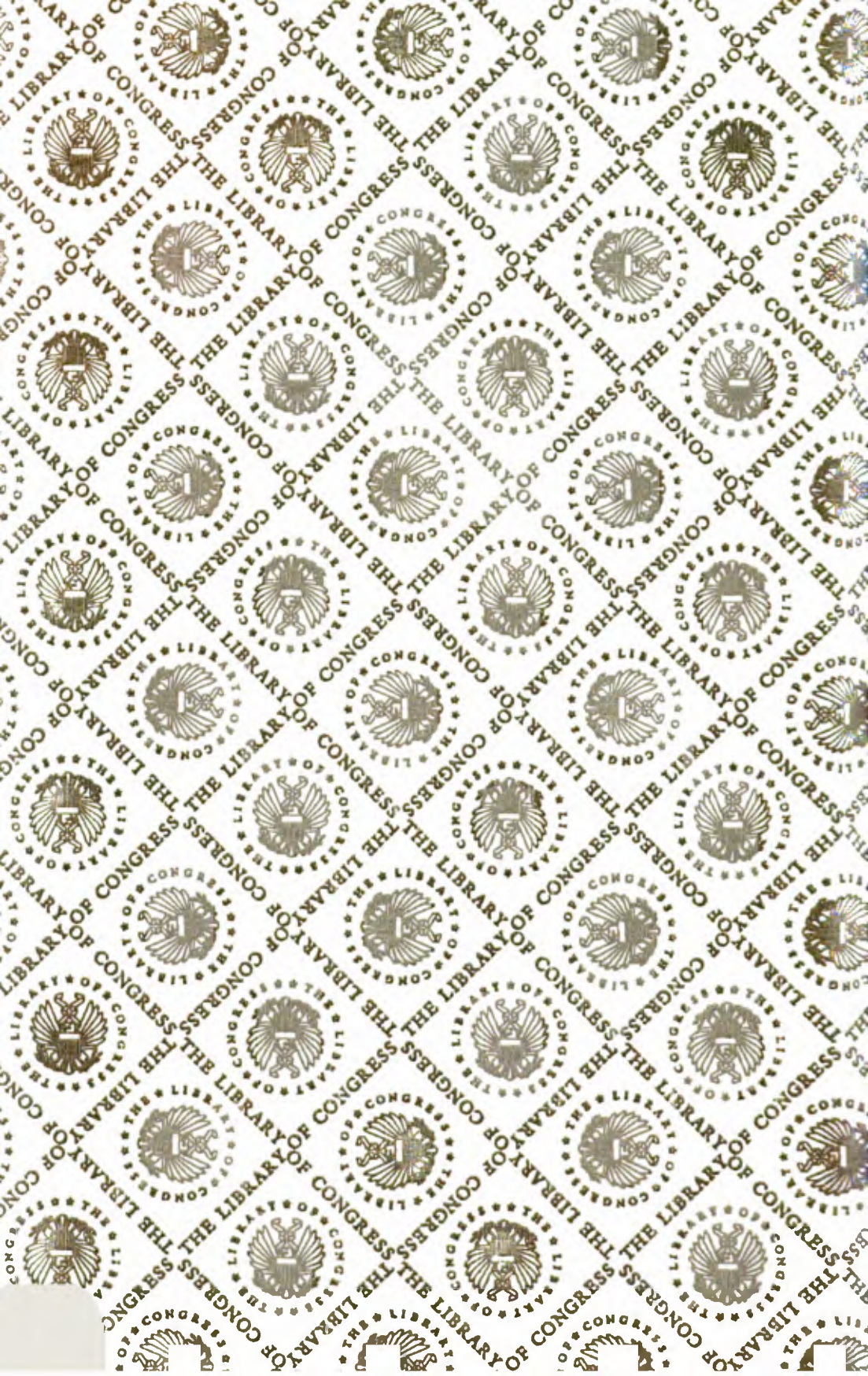
[48] See, *Encryption, Key Recovery & Law Enforcement: Selected Legal Issues and Legislative Proposals*, Library of Congress, Congressional Research Service, by Charles Doyle, Sep. 12, 1997.

[49] U.S. Congress, Office of Technology Assessment, *Issue Update on Information Security and Privacy in Network Environments* at 7, OTA-BP-ITC-147 (Washington, D.C: U.S. Government Printing Office, June 1995).

[50] See, *Encryption Export Controls*, Library of Congress, Congressional Research Service, Rep. No. 97-837A by Jeanne J. Grimmett, Sep. 15, 1997.

[51] See, *Encryption Technology: Congressional Issues*, Library of COngress, Congressional Research Service, IB96039 by Marcia Smith, Sep. 11, 1997.

○


THE LIBRARY OF CONGRESS